$(2n,r,t)$_GFNSP 结构一类不可能差分对的构造方法

崔　霆*　　金晨辉
(信息工程大学电子技术学院　郑州　450004)

摘　要：构造不可能差分对是进行不可能差分分析的前提。该文研究了 $(2n,r,t)$_GFNSP 结构不可能差分对的构造问题，给出了该结构的一类$(4n+1)$轮不可能差分对的结构形式以及计算复杂度为 $O(n^2r^{10})$的构造算法，针对 Shirai 等提出的 $(2n,r,t)$_GFNSP 结构的 DSM 设计策略，本文给出了相应的$(4n+1)$轮不可能差分对的构造方法。

关键词：分组密码；$(2n,r,t)$_GFNSP 结构；不可能差分对；扩散结构；分支数
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2011)01-0194-05
DOI: 10.3724/SP.J.1146.2009.01494

A Construction Method of Impossible Difference for $(2n,r,t)$_GFNSP Overall Structure

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

Abstract: Impossible differential attack should be launched with the construction of impossible difference. This paper investigates the construction method of impossible differences for $(2n,r,t)$_GFNSP overall structure. A kind of $(4n+1)$-round impossible differences and the construct method with computation complexity $O(n^2r^{10})$ are presented. And this paper provides the structure of $(4n+1)$-round impossible differences against the DSM strategy which is proposed by Shirai *et al*..

Key words: Block cipher; $(2n,r,t)$_GFNSP overall structure; Impossible difference; Diffusion layer; Branch number

1　引言

不可能差分攻击[1]是分组密码的一类重要的攻击方法，该方法利用一条或者多条概率为0的差分对来完成对正确密钥的筛选工作，这里的概率为0的差分对称作不可能差分对。从不可能差分攻击提出至今，密码分析者们利用这一攻击方法对诸如 Skipjack[1]，AES[2]，Camellia[3]，ARIA[3]，CLEFIA[4−6]等大量分组密码算法实施了有效的分析。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对。更进一步地，如果能够给出一个算法结构不可能差分对的构造方法[7,8]，那么对所有利用该结构设计的密码算法，我们均可以方便地进行不可能差分分析。因此，给出算法结构的不可能差分对的构造方法意义更显重大。值得指出的是，目前该领域的结果并不多见。

本文将考察一类嵌套SP结构的广义Feistel结构[9](即 $(2n,r,t)$_GFNSP 结构)不可能差分对的构造问题，给出 $(2n,r,t)$_GFNSP 结构的$4n+1$轮不可能差分对的结构形式及相应的复杂度为$O(n^2r^{10})$的构造方法。文献[10,11]提出了DSM策略来优化设计 $(2n,r,t)$_GFNSP 结构的扩散结构，并设计了CLEFIA算法[12]。针对这一设计策略，本文将进一步给出相应的$4n+1$轮不可能差分对的构造方法。

2　预备知识

本文若无特别说明，均以“$\oplus$”表示逐位异或运算，以“+”表示实数加法，$\#S$ 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；本文中所有的计数均始于 1。

定义 1[9]　如果密码算法的轮函数 Q_k 满足

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

其中 $f_1,f_2,\cdots,f_n$ 均为 $\{0,1\}^m\times\{0,1\}^m\to\{0,1\}^m$ 的变换，依次称之为第 1 至第 n 个 F 函数。k 为轮子密钥。则称该结构为 $2n$ 分组的广义 Feistel 结构，简记作 $(2n,m)$_GFN 结构。分别称 x_i,y_i 为轮函数的第 i 个输入、输出块。

备注 1　各参数同定义 1，$(2n,m)$_GFN 结构的逆轮函数 Q_k^{-1} 为

2009-11-20 收到，2010-09-07 改回
*通信作者：崔霆　cuiting_1209@yahoo.com.cn

$$(x_1,x_2,\cdots,x_{2n})=Q_k^{-1}(y_1,y_2,\cdots,y_{2n})=(y_{2n},y_1\oplus f_1(k,y_{2n}),y_2,y_3\oplus f_2(k,y_2),\cdots,y_{2n-2},y_{2n-1}\oplus f_n(k,y_{2n-2}))$$

定义 2　在 $(2n,rt)$_GFN 结构中，$i=1,2,\cdots,n$ 时，若各 F 函数均满足 $f_i(x)=P_iS_i(x\oplus k)$，这里 k 是与输入 x 等长的圈子密钥；$S_i(\boldsymbol{y})=(s_{i1}(y_1),s_{i2}(y_2),\cdots,s_{ir}(y_r))$，对 $1\le j\le r$，s_{ij} 均为 $\{0,1\}^t\to\{0,1\}^t$ 的非线性置换；诸 P_i 均为 $\mathrm{GF}(2^t)^r\to\mathrm{GF}(2^t)^r$ 的线性变换，即 $P_i(\boldsymbol{y})=\boldsymbol{M}_i\boldsymbol{y}$，这里 $\boldsymbol{M}_i$ 为 P_i 的矩阵表示，$\boldsymbol{y}$ 为列向量。则称该结构为 $2n$ 分组嵌套 SP 结构的广义 Feistel 结构，记为 $(2n,r,t)$_GFNSP。

定义 3　设 $(X,+)$ 和 $(Y,+)$ 都是有限交换群，$f:X\to Y,\Delta x\in X,\ \Delta y\in Y$，令

$$p_f(\Delta x\to\Delta y)=\frac{1}{\#X}\#\{x\in X:f(x+\Delta x)-f(x)=\Delta y\}$$

则称 $\Delta x\to\Delta y$ 为 f 的一个差分对应，称 $p_f(\Delta x\to\Delta y)$ 为该差分对应的转移概率。为方便起见，以下用 $\Delta_f(\Delta x)$ 表示输入差为 Δx 时 f 的输出差。

不难看出，当 f 是 $\mathrm{GF}(2^n)^m$ 上的线性变换时，有 $\Delta_f(\Delta\boldsymbol{x})=f(\Delta\boldsymbol{x})$；当 f 是双射时，$\Delta_f(\Delta\boldsymbol{x})=0$ 当且仅当 $\Delta\boldsymbol{x}=0$。

定义 4　设 $x\in\mathrm{GF}(2^n)$，定义特征变换 $\chi_n:\mathrm{GF}(2^n)\to\mathrm{GF}(2)$ 为

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

通常，若 $\boldsymbol{X}=(x_1,\cdots,x_m)\in\mathrm{GF}(2^n)^m$，也用 $\chi_n(\boldsymbol{X})$ 表示 $(\chi_n(x_1),\cdots,\chi_n(x_m))$。

定义 5　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 $\boldsymbol{A}$ 的差分分支数为

$$B_d=\min\{W(\boldsymbol{\alpha})+W(\boldsymbol{A\alpha}):\boldsymbol{\alpha}\in[\mathrm{GF}(2^n)]^t\setminus\{0\}\}$$

3　$(2n,r,t)$_GFNSP 结构 $4n+1$ 轮不可能差分对的构造

首先本文将分析 $(2n,m)$_GFN 结构的差分传播规律。以下约定 $(2n,m)$_GFN 结构的第 i 轮、第 s 块的输入差分为 Δx_s^i。

定理1　$(2n,m)$_GFN 结构加密变换的一轮差分对应必具有

$$(\Delta x_1,\Delta x_2,\cdots,\Delta x_{2n})\to(\Delta x_2\oplus\beta_1,\Delta x_3,\cdots,\Delta x_{2n}\oplus\beta_n,\Delta x_1)$$

的形式，且

$$p_{Q_k}((\Delta x_1,\Delta x_2,\cdots,\Delta x_{2n})\to(\Delta x_2\oplus\beta_1,\Delta x_3,\cdots,\Delta x_{2n}\oplus\beta_n,\Delta x_1))=\prod_{t=1}^{n}p_{f_t}(\Delta x_{2t-1}\to\beta_t)$$

证明　$\forall(\Delta x_1,\Delta x_2,\cdots,\Delta x_{2n})$ 由于

$$\begin{aligned}&Q_k(x_1,x_2,\cdots,x_{2n})\oplus Q_k(x_1\oplus\Delta x_1,x_2\oplus\Delta x_2,\cdots,x_{2n}\oplus\Delta x_{2n})\\&=(x_2\oplus f_1(k,x_1),x_3,\cdots,x_{2n}\oplus f_n(k,x_{2n-1}),x_1)\oplus(x_2\oplus\Delta x_2\oplus f_1(k,x_1\oplus\Delta x_1),x_3\oplus\Delta x_3,\cdots,x_{2n}\oplus\Delta x_{2n}\oplus f_n(k,x_{2n-1}\oplus\Delta x_{2n-1}),x_1\oplus\Delta x_1)\\&=(\Delta x_2\oplus f_1(k,x_1\oplus\Delta x_1)\oplus f_1(k,x_1),\Delta x_3,\cdots,\Delta x_{2n}\oplus f_n(k,x_{2n-1})\oplus f_n(k,x_{2n-1}\oplus\Delta x_{2n-1}),\Delta x_1)\\&=(\Delta x_2\oplus\beta_1,\Delta x_3,\cdots,\Delta x_{2n}\oplus\beta_n,\Delta x_1)\end{aligned}$$

这里，对 $t=1,2,\cdots,n$，均设 $f_t(k,x_{2t-1}\oplus\Delta x_{2t-1})\oplus f_t(k,x_{2t-1})=\beta_t$。从而

$$p_{Q_k}((\Delta x_1,\Delta x_2,\cdots,\Delta x_{2n})\to(\Delta x_2\oplus\beta_1,\Delta x_3,\cdots,\Delta x_{2n}\oplus\beta_n,\Delta x_1))=\prod_{t=1}^{n}p_{f_t}(\Delta x_{2t-1}\to\beta_t)$$

证毕

由定理1可以容易地得到下面的推论。

推论1　若 $(2n,m)$_GFN 结构的一轮差分对为

$$(\Delta x_1^i,\Delta x_2^i,\cdots,\Delta x_{2n}^i)\to(\Delta x_1^{i+1},\Delta x_2^{i+1},\cdots,\Delta x_{2n}^{i+1})$$

则对 $1\le t\le n$，均有 $\Delta x_{2t}^{i+1}=\Delta x_{2t+1(\bmod 2n)}^i$ 和 $\Delta x_{2t-1}^{i+1}=\Delta f_t(\Delta x_{2t-1}^i)\oplus\Delta x_{2t}^i$ 成立。

类似地，可以得到 $(2n,m)$_GFN 结构脱密变换的差分对应形式。

定理2　$(2n,m)$_GFN 结构脱密变换的一轮差分对应必具有

$$(\Delta y_1,\Delta y_2,\cdots,\Delta y_{2n})\to(\Delta y_{2n},\Delta y_1\oplus\gamma_1,\cdots,\Delta y_{2n-2},\Delta y_{2n-1}\oplus\gamma_n)$$

的形式，且

$$p_{Q_k^{-1}}((\Delta y_1,\Delta y_2,\cdots,\Delta y_{2n})\to(\Delta y_{2n},\Delta y_1\oplus\gamma_1,\cdots,\Delta y_{2n-1}\oplus\gamma_n))=p_{f_1}(\Delta y_{2n}\to\gamma_1)\times\prod_{t=2}^{n}p_{f_t}(\Delta y_{2t-2}\to\gamma_t)$$

证明　$\forall(\Delta y_1,\Delta y_2,\cdots,\Delta y_{2n})$ 由于

$$\begin{aligned}&Q_k^{-1}(y_1,y_2,\cdots,y_{2n})\oplus Q_k^{-1}(y_1\oplus\Delta y_1,y_2\oplus\Delta y_2,\cdots,y_{2n}\oplus\Delta y_{2n})=(y_{2n},y_1\oplus f_1(k,y_{2n}),\cdots,y_{2n-2},y_{2n-1}\oplus f_n(k,y_{2n-2}))\oplus(y_{2n}\oplus\Delta y_{2n},y_1\oplus\Delta y_1\oplus f_1(k,y_{2n}\oplus\Delta y_{2n}),\cdots,y_{2n-2}\oplus\Delta y_{2n-2},y_{2n-1}\oplus\Delta y_{2n-1}\oplus f_n(k,y_{2n-2}\oplus\Delta y_{2n-2}))=(\Delta y_{2n},\Delta y_1\oplus f_1(k,y_{2n}\oplus\Delta y_{2n})\oplus f_1(k,y_{2n}),\cdots,\Delta y_{2n-2},\Delta y_{2n-1}\oplus f_n(k,y_{2n-2})\oplus f_n(k,y_{2n-2}\oplus\Delta y_{2n-2}))=(\Delta y_{2n},\Delta y_1\oplus\gamma_1,\cdots,\Delta y_{2n-2},\Delta y_{2n-1}\oplus\gamma_n)\end{aligned}$$

这里设 $f_1(k,y_{2n}\oplus\Delta y_{2n})\oplus f_1(k,y_{2n})=\gamma_1$，且对 $t=2,\cdots,n$，设 $f_t(k,y_{2t-2})\oplus f_t(k,y_{2t-2}\oplus\Delta y_{2t-2})=\gamma_t$。从而

$$p_{Q_k^{-1}}((\Delta y_1,\Delta y_2,\cdots,\Delta y_{2n})\to(\Delta y_{2n},\Delta y_1\oplus\gamma_1,\cdots,\Delta y_{2n-1}\oplus\gamma_n))=p_{f_1}(\Delta y_{2n}\to\gamma_1)\times\prod_{t=2}^{n}p_{f_t}(\Delta y_{2t-2}\to\gamma_t)$$

证毕

同样地，下面的推论成立。

推论2 若 $(2n,m)_$GFN 结构逆变换的一轮差分对为

$$(\Delta y_1^i,\Delta y_2^i,\cdots,\Delta y_{2n}^i)\to(\Delta y_1^{i+1},\Delta y_2^{i+1},\cdots,\Delta y_{2n}^{i+1})$$

则有 $\Delta y_1^{i+1}=\Delta y_{2n}^i$ 和 $\Delta y_2^{i+1}=f(\Delta y_{2n}^i)\oplus\Delta y_1^i$，且对 $1\le t\le n-1$ 均有 $\Delta y_{2t+1}^{i+1}=\Delta y_{2t}^i$ 和 $\Delta y_{2t}^{i+1}=f_t(\Delta y_{2t-2}^i)\oplus\Delta y_{2t-1}^i$ 成立。

定理3 $(2n,r,t)_$GFNSP 结构的各F函数P变换的矩阵表示依次设为 $\boldsymbol{M}_1,\boldsymbol{M}_2,\cdots,\boldsymbol{M}_n$，若首轮输入差仅 $\Delta\boldsymbol{x}_{2s}^1$ 非0，则 $\Delta\boldsymbol{x}_{2s}^{2n+2}$ 必具有形式 $\overset{n}{\underset{i=1}{\oplus}}\boldsymbol{M}_i\Delta\boldsymbol{x}_{2s\_i}^1$。这里诸 $\Delta\boldsymbol{x}_{2s\_i}^1$ 满足 $\chi_t(\Delta\boldsymbol{x}_{2s\_1}^1)=\chi_t(\Delta\boldsymbol{x}_{2s\_2}^1)=\cdots=\chi_t(\Delta\boldsymbol{x}_{2s\_n}^1)=\chi_t(\Delta\boldsymbol{x}_{2s}^1)$。

证明 不妨设 $(2n,r,t)_$GFNSP 结构的首轮输入差分为 $(0,0,\cdots,0,\Delta\boldsymbol{x}_{2s}^1,0,\cdots,0)$，$\Delta\boldsymbol{x}_{2s}^1\ne0$，则由推论1，形象地，可以以概率1得到差分传递链如表1所示，这里0表示全0差分，“*”表示不确定的差分。

表1 差分传递链

块数	1	2	…	$(2s-2)$	$(2s-1)$	$2s$	$(2s+1)$	…	$(2n-1)$	$2n$
圈数\输出差	0	0	…	0	0	$\Delta\boldsymbol{x}_{2s}^1$	0	…	0	0
1	0	0	…	0	$\Delta\boldsymbol{x}_{2s}^1$	0	0	…	0	0
2	0	0	…	$\Delta\boldsymbol{x}_{2s}^1$	$\Delta_{f_1}(\Delta\boldsymbol{x}_{2s}^1)$	0	0	…	0	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
$(2s-1)$	$\Delta\boldsymbol{x}_{2s}^1$	$\overset{s}{\underset{i=2}{\oplus}}\Delta_{f_i}(\Delta\boldsymbol{x}_{2s}^1)$	…	*	*	0	0	…	0	0
$2s$	$\overset{s}{\underset{i=1}{\oplus}}\Delta_{f_i}(\Delta\boldsymbol{x}_{2s}^1)$	*	…	*	*	0	0	…	0	$\Delta\boldsymbol{x}_{2s}^1$
$(2s+1)$	*	*	…	*	*	0	0	…	$\Delta\boldsymbol{x}_{2s}^1$	$\overset{s}{\underset{i=1}{\oplus}}\Delta_{f_i}(\Delta\boldsymbol{x}_{2s}^1)$
$(2s+2)$	*	*	…	*	*	0	0	…	$\overset{s}{\underset{i=1}{\oplus}}\Delta_{f_i}(\Delta\boldsymbol{x}_{2s}^1)\oplus\Delta_{f_s}(\Delta\boldsymbol{x}_{2s}^1)$	*
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
$2n$	*	*	…	*	*	$\Delta\boldsymbol{x}_{2s}^1$	$\overset{n}{\underset{i=1}{\oplus}}\Delta_{f_i}(\Delta\boldsymbol{x}_{2s}^1)$	…	*	*
$(2n+1)$	*	*	…	*	*	$\overset{n}{\underset{i=1}{\oplus}}\Delta_{f_i}(\Delta\boldsymbol{x}_{2s}^1)$	*	…	*	*

由上面的差分传递链知，第 $(2n+2)$ 轮的第 $2s$ 块输入差分，$\Delta\boldsymbol{x}_{2s}^{2n+2}=\overset{n}{\underset{i=1}{\oplus}}\Delta f_i(\Delta\boldsymbol{x}_{2s}^1)=\overset{n}{\underset{i=1}{\oplus}}\Delta_{P_iS_i}(\Delta\boldsymbol{x}_{2s}^1)=\overset{n}{\underset{i=1}{\oplus}}\Delta_{P_i}[\Delta_{S_i}(\Delta\boldsymbol{x}_{2s}^1)]$，又，在 $(2n,r,t)_$GFNSP 结构中，所有的 S_i 均是由 r 个 t 比特非线性双射并置构成的，故 $\chi_t(\Delta_{S_i}(\Delta\boldsymbol{x}_{2s}^1))=\chi_t(\Delta\boldsymbol{x}_{2s}^1)$，若记 $\Delta_{S_i}(\Delta\boldsymbol{x}_{2s}^1)=\Delta\boldsymbol{x}_{2s\_i}^1$，则 $\Delta\boldsymbol{x}_{2s}^{2n+2}=\overset{n}{\underset{i=1}{\oplus}}\Delta_{P_i}[\Delta_{S_i}(\Delta\boldsymbol{x}_{2s}^1)]=\overset{n}{\underset{i=1}{\oplus}}\Delta_{P_i}(\Delta\boldsymbol{x}_{2s\_i}^1)$，而诸 P_i 为线性变换，且其矩阵表示依次为 $\boldsymbol{M}_1,\boldsymbol{M}_2,\cdots,\boldsymbol{M}_n$，故 $\Delta\boldsymbol{x}_{2s}^{2n+2}=\overset{n}{\underset{i=1}{\oplus}}\Delta_{P_i}(\Delta\boldsymbol{x}_{2s\_i}^1)=\overset{n}{\underset{i=1}{\oplus}}\boldsymbol{M}_i\Delta\boldsymbol{x}_{2s\_i}^1$。 证毕

与定理3的推导过程完全类似，根据推论2考察 $(2n,r,t)_$GFNSP 的逆变换，可以得到下面的结论。

定理4 $(2n,r,t)_$GFNSP 结构的各F函数P变换的矩阵表示依次设为 $\boldsymbol{M}_1,\boldsymbol{M}_2,\cdots,\boldsymbol{M}_n$。若第 $2n$ 轮输出差仅 $\Delta\boldsymbol{x}_{2s-1}^{2n+1}$ 非0，则 $\Delta\boldsymbol{x}_{2s}^1$ 必具有形式 $\overset{n}{\underset{i=1}{\oplus}}\boldsymbol{M}_i\Delta\boldsymbol{x}_{2s-1\_i}^{2n+1}$。这里诸 $\Delta\boldsymbol{x}_{2s-1\_i}^{2n+1}$ 满足 $\chi_t(\Delta\boldsymbol{x}_{2s-1\_1}^{2n+1})=\chi_t(\Delta\boldsymbol{x}_{2s-1\_2}^{2n+1})=\cdots=\chi_t(\Delta\boldsymbol{x}_{2s-1\_n}^{2n+1})=\chi_t(\Delta\boldsymbol{x}_{2s-1}^{2n+1})$。

由定理3及定理4，以下结论成立。

定理5 $(2n,r,t)_$GFNSP 结构的各F函数P变换矩阵表示依次设为 $\boldsymbol{M}_1,\boldsymbol{M}_2,\cdots,\boldsymbol{M}_n$，若抽出 $\boldsymbol{M}_1,\boldsymbol{M}_2,\cdots,\boldsymbol{M}_n$ 的第 $i_1,i_2,\cdots,i_m$ 列后所得的 mn 个向量线性无关，且 $\forall\Delta\boldsymbol{x}_{2s}^1,\Delta\boldsymbol{x}_{2s-1}^{4n+2}\in\mathrm{GF}(2^t)^r$，若 $\Delta\boldsymbol{x}_{2s}^1$，$\Delta\boldsymbol{x}_{2s-1}^{4n+2}$ 除第 $i_1,i_2,\cdots,i_m$ 分量之外均为0，则

$$(0,0,\cdots,0,\Delta\boldsymbol{x}_{2s}^1,0\cdots,0)\xrightarrow{(4n+1)\text{ round}}(0,0,\cdots,0,\Delta\boldsymbol{x}_{2s-1}^{4n+2},0\cdots,0)$$

一定是 $(2n,r,t)_$GFNSP 结构的不可能差分。

证明 由定理3知，若第1轮输入差为 $(0,0,\cdots,0,\Delta\boldsymbol{x}_{2s}^1,0\cdots,0)$，则有 $\Delta\boldsymbol{x}_{2s}^{2n+2}=\overset{n}{\underset{i=1}{\oplus}}\boldsymbol{M}_i\Delta\boldsymbol{x}_{2s\_i}^1$，这里对 $1\le i\le n$ 均有 $\chi_t(\Delta\boldsymbol{x}_{2s\_i}^1)=\chi_t(\Delta\boldsymbol{x}_{2s}^1)$。由定理4知，若第 $(4n+1)$ 轮输出差为 $(0,0,\cdots,0,\Delta\boldsymbol{x}_{2s-1}^{4n+2},0\cdots,0)$，则有 $\Delta\boldsymbol{x}_{2s}^{2n+2}=\overset{n}{\underset{i=1}{\oplus}}\boldsymbol{M}_i\Delta\boldsymbol{x}_{2s-1\_i}^{4n+2}$，这里对 $1\le i\le n$ 均有 $\chi_t(\Delta\boldsymbol{x}_{2s-1\_i}^{4n+2})=\chi_t(\Delta\boldsymbol{x}_{2s-1}^{4n+2})$。形象地，有前 $(2n+1)$ 轮差分对应关系

$$(0,0,\cdots,0,\Delta\boldsymbol{x}_{2s}^1,0\cdots,0)\xrightarrow{(2n+1)\text{ round}}\Delta\boldsymbol{x}_{2s}^{2n+2}=\overset{n}{\underset{i=1}{\oplus}}\boldsymbol{M}_i\Delta\boldsymbol{x}_{2s\_i}^1$$

和后$2n$圈差分对应关系

$$\Delta \boldsymbol{x}_{2s}^{2n+2}=\overset{n}{\underset{i=1}{\oplus}}\boldsymbol{M}_i\Delta \boldsymbol{x}_{2s-1\_i}^{4n+2}\xleftarrow{2n\ \text{round}}\left(0,0,\cdots,0,\Delta \boldsymbol{x}_{2s-1}^{4n+2},0\cdots,0\right)$$

故差分对应$(0,0,\cdots,0,\Delta \boldsymbol{x}_{2s}^{1},0\cdots,0)\xrightarrow{(4n+1)\ \text{round}}(0,0,\cdots,0,\Delta \boldsymbol{x}_{2s-1}^{4n+2},0\cdots,0)$成立的必要条件为$\overset{n}{\underset{i=1}{\oplus}}\boldsymbol{M}_i\Delta x_{2s_i}^{1}=\overset{n}{\underset{i=1}{\oplus}}\boldsymbol{M}_i\Delta x_{2s-1_i}^{4n+2}$成立，即$\overset{n}{\underset{i=1}{\oplus}}\boldsymbol{M}_i(\Delta \boldsymbol{x}_{2s_i}^{1}\oplus\Delta \boldsymbol{x}_{2s-1_i}^{4n+2})=0$。但因$\Delta \boldsymbol{x}_{2s_i}^{1}$，$\Delta \boldsymbol{x}_{2s-1_i}^{4n+2}$除第$i_1,i_2,\cdots,i_m$块之外均为0，故$\Delta \boldsymbol{x}_{2s_i}^{1}\oplus\Delta \boldsymbol{x}_{2s-1_i}^{4n+2}$至多只能在第$i_1,i_2,\cdots,i_m$个分量处非零。又知$\boldsymbol{M}_1,\boldsymbol{M}_2,\cdots,\boldsymbol{M}_n$的第$i_1,i_2,\cdots,i_m$列线性无关。故一定有$\overset{n}{\underset{i=1}{\oplus}}\boldsymbol{M}_i\left(\Delta \boldsymbol{x}_{2s_i}^{1}\oplus\Delta \boldsymbol{x}_{2s-1_i}^{4n+2}\right)\neq 0$，即$(0,0,\cdots,0,\Delta \boldsymbol{x}_{2s}^{1},0\cdots,0)\xrightarrow{(4n+1)\ \text{round}}(0,0,\cdots,0,\Delta \boldsymbol{x}_{2s-1}^{4n+2},0,\cdots,0)$是$(2n,r,t)$_ GFNSP 结构的不可能差分。证毕

推论 3　若差分对应$(0,0,\cdots,0,\Delta \boldsymbol{x},0\cdots,0)\xrightarrow{(4n+1)\ \text{round}}(0,0,\cdots,0,\Delta \boldsymbol{y},0\cdots,0)$是定理5所构造$(2n,r,t)$_GFNSP 结构的$(4n+1)$轮不可能差分，则$\Delta \boldsymbol{x}$和$\Delta \boldsymbol{y}$中至多各有$\lfloor r/n\rfloor$块非0。这里$\lfloor a\rfloor$表示对$a$的下取整。

定义6　设$\boldsymbol{\eta}_1,\boldsymbol{\eta}_2$均为$r$维0–1向量，若$\boldsymbol{\eta}_2$在$\boldsymbol{\eta}_1$的所有为0比特处均为0，则称$\boldsymbol{\eta}_1$包含$\boldsymbol{\eta}_2$，或$\boldsymbol{\eta}_2$包含于$\boldsymbol{\eta}_1$。

由此可以得到构造$(2n,r,t)$_GFNSP 结构的一类$(4n+1)$轮不可能差分的算法如表2所示。

表 2 中步骤 1 需要 2 个指令；步骤 2 需要约$\sum_{k=1}^{a}C_r^k$条指令；步骤 3 需要约$r^4\times n^2\times\sum_{k=1}^{a}C_r^k\times C_{C_r^2}^{2}$条指令。故算法 1 的计算复杂度为约为$O(n^2r^{10})$。

文献[10,11]提出了针对Feistel结构的DSM设计策略，即建议各轮的扩散结构采用级联后分支数较大的矩阵来设计Feistel结构中F函数的P盒。文献[12]将这一策略应用于$(2n,r,t)$_GFNSP 结构，并设计了CLEFIA算法。对此有以下的推论。

推论4　在$(2n,r,t)$_GFNSP 结构中，若各轮函数的扩散结构的矩阵表示$\boldsymbol{M}_1,\boldsymbol{M}_2,\cdots,\boldsymbol{M}_n$满足$B_d(\boldsymbol{M}_1\mid\boldsymbol{M}_2\mid\cdots\mid\boldsymbol{M}_n)=d$，$r$维非零向量$\Delta \boldsymbol{x}_{2s}^{1}$，$\Delta \boldsymbol{x}_{2s-1}^{4n+2}$满足$\chi_t(\Delta \boldsymbol{x}_{2s}^{1}),\chi_t(\Delta \boldsymbol{x}_{2s-1}^{4n+2})$包含于$\boldsymbol{\alpha}$，则差分对应$(0,0,\cdots,0,\Delta \boldsymbol{x}_{2s}^{1},0\cdots,0)\xrightarrow{(4n+1)\ \text{round}}(0,0,\cdots,0,\Delta \boldsymbol{x}_{2s-1}^{4n+2},0\cdots,0)$均为$(2n,r,t)$_GFNSP 的$4n+1$轮不可能差分。这里，$\boldsymbol{\alpha}$是满足$W(\boldsymbol{\alpha})<d/n$的任意的非零$r$维0–1向量。

证明　由$B_d(\boldsymbol{M}_1\mid\boldsymbol{M}_2\mid\cdots\mid\boldsymbol{M}_n)=d$知，任意抽出$\boldsymbol{M}_1,\boldsymbol{M}_2,\cdots,\boldsymbol{M}_n$的不多于$W(\boldsymbol{\alpha})$列后所得的$n\times W(\boldsymbol{\alpha})$个向量线性无关，由定理5，结论成立。

证毕

表2 $(2n,r,t)$_GFNSP结构的一类$(4n+1)$轮不可能差分算法

输入 (1) $(2n,r,t)$_GFNSP 的扩散结构的矩阵表示$\boldsymbol{M}_1,\boldsymbol{M}_2,\cdots,\boldsymbol{M}_n$；

(2)扩散结构定义的有限域GF(2^t) 的乘法表。

输出　$(2n,r,t)$_GFNSP 的$(4n+1)$轮不可能差分。

步骤1　计算$a=\lfloor r/n\rfloor$，若$a=0$，输出：构造失败，程序结束，否则进行步骤2；

步骤2　构造Ω为所有重量不大于a的非零r维0–1向量集合；

步骤3　对Ω中的每一个向量$\boldsymbol{\beta}$，进行下列操作：

步骤3.1　令$m=0$;

```
for(i = 0; i < r; i++)
{
  if(β >> i)%2 == 1)
{
抽取 M_1, M_2, ..., M_n 的第i列，存放于 A[m][n] 中；
m++;
}
}
```

步骤3.2　判断数组$\boldsymbol{A}$在GF(2^t) 上是否满秩，若不满秩，则退回步骤3。若$\boldsymbol{A}$满秩，则对每一对满足$(\chi_t(\Delta \boldsymbol{x})\mid\chi_t(\Delta \boldsymbol{y}))$包含于$\boldsymbol{\beta}$的$(\Delta \boldsymbol{x}\mid\Delta \boldsymbol{y})$，进行下面的操作。

```
for(s = 1; s ≤ n; s++)
{
  Δx^1_{2s} ← Δx; Δx^{4n+2}_{2s-1} ← Δy ;
  输出 (0,0,...,0,Δx^1_{2s},0...,0) --(4n+1) round--> (0,0,...,0,Δx^{4n+2}_{2s-1},0...,0) ;
}
```

若步骤3已经遍历完成，则程序结束；否则返回步骤3，进行下一次遍历。

从推论 4 不难看出，当n=1 时，必然存在 5 轮不可能差分对，当 n=2 时，只要$d>4$，则一定存在 9 轮不可能差分对。当d取最大值$(r+1)$时，只要同时有$2n\le r+1$，就必然存在$(4n+1)$轮不可能差分对。值得指出的是，利用该推论可以得到文献[4–6]中所有关于 CLEFIA 算法的不可能差分对。

4　结束语

不可能差分分析是密码分析学研究的热点之一，而不可能差分对的构造是其中的核心内容。本文研究了$(2n,r,t)$_GFNSP 结构不可能差分对的构造问题，给出该结构的$(4n+1)$轮不可能差分对的结构形式及计算复杂度为$O(n^2r^{10})$的$(4n+1)$轮不可能差分对的构造方法，并针对 DSM 设计策略，给出$(2n,r,t)$_GFNSP 结构相应的不可能差分对的构造

方法。利用本文的结果，可以得到文献[4–6]中所有关于 CLEFIA 算法的不可能差分对。如何给出 $(2n,r,t)_$GFNSP 结构的其他类型的不可能差分的形式，以及如何给出其它结构的不可能差分对，是今后需要深入的问题。

参 考 文 献

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

[2] Zhang Wen-tao, Wu Wen-ling, and Zhang Lei, *et al*.. Improved related-key impossible differential attacks on reduced-round AES-192[C]. Proceedings of Selected Areas in Cryptography 2006, LNCS 4356: 15–27.

[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] Tsunoo Y, Tsujihara E, and Shigeri M, *et al*.. Impossible differential cryptanalysis of CLEFIA. FSE2008, LNCS 5086: 398–411.

[5] Sun Bing, Li Rui-lin, and Wang Mian, *et al*.. Impossible differential cryptanalysis of CLEFIA. Cryptology ePrint Archive, Report, 2008: 151.

[6] Wang Wei and Wang Xiao-yun. Improved impossible differential cryptanalysis of CLEFIA. Cryptology ePrint Archive, Report, 2007: 466.

[7] Wu Wen-ling, Zhang Lei, and Zhang Li-ting, *et al*.. Security analysis of the GF-NLFSR structure and four-cell Block Cipher[C]. ICICS 2009, LNCS 5927: 17–31.

[8] Li Rui-lin, Sun Bing, and Li Chao. Distinguishing attacks on a kind of generalized unbalanced feistel network. Cryptology ePrint Archive, Report, 2009: 360.

[9] Zheng Y, Matsumoto T, and Imai H. On the construction of block ciphers provably secure and not relying on any unproved hypotheses[C]. CRYPTO 1989, LNCS 435: 461–480.

[10] Shirai T and Preneel B. On Feistel ciphers using optimal diffusion mappings across multiple rounds[C]. ASIACRYPT 2004, LNCS 3329: 1–15.

[11] Shirai T and Shibutani K. On Feistel structures using a diffusion switching mechanism[C]. FSE 2006, LNCS 4047: 41–56.

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

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，博士生导师，研究方向为密码学与信息安全.