文章编号:1000－2367(2015)05－0142－05 DOI:10.16366/j.cnki.1000－2367.2015.05.027

一类扩展广义 Feistel 结构的活动轮函数个数的下界

殷 勍,王念平

(解放军信息工程大学 密码工程学院,郑州 450000)

摘 要:扩展广义 Feistel 结构是近期提出的一类分组密码结构,为评估该类密码结构的安全性能,对 4 分组扩展广义 Feistel 结构抵抗差分密码分析的能力进行了详细的研究.在轮函数为双射的假设条件下,给出了任意轮差分特征中活动轮函数个数的下界.

关键词:展广义 Feistel 结构;差分密码分析;活动轮函数;下界

中图分类号:TN918.2 **文献标志码**:A

广义 Feistel 结构[1－2]是常用的分组密码整体结构之一,其一经提出就受到人们的广泛关注[3－6].有许多分组密码都采用了广义 Feistel 结构,例如 CAST-256[7],RC6[8],CLEFIA[9]以及 MARS[10]等.为了实现方便,广义 Feistel 结构一般使用循环移位作为其扩散层变换.Suzaki[11]与 Yanagihara[12]等人分别指出,用特定的置换代替循环移位可以获得更好的扩散效果.Berger[13]等人在文献[11－12]的基础上提出扩展广义 Feistel 结构,并声称该结构的扩散效果更好.

在文献[13]中,作者针对输入分成 8 个分块和 16 个分块的情形,对扩展广义 Feistel 结构抵抗常见密码分析方法的能力进行了估计,但对于输入分成 4 个分块的情形,并没有给出相应的结论.众所周知,差分密码分析[14]是攻击分组密码的强有力的工具,估计分组密码抵抗这种攻击的能力是必须考虑的问题.基于此,本文针对输入分成 4 个分块的情形,详细研究了扩展广义 Feistel 结构抵抗差分密码分析的能力.文献[15]指出,如果分组密码的最大差分特征概率足够小,就可以认为该密码对差分密码分析是实际安全的,而最大差分特征概率通常又可以用差分特征中活动轮函数个数的下界来估计,从而,估计分组密码抵抗差分密码分析能力的关键是找出活动轮函数个数的下界.按照这种思路,本文针对输入分成 4 个分块的情形,给出了多轮差分特征中活动轮函数个数的下界.为叙述方便起见,称输入分成 4 个分块的扩展广义 Feistel 结构为"4 分组扩展广义 Feistel 结构".

1 预备知识

1.1 基本概念

定义 1[16] 设$(X,+)$和$(Y,+)$都是有限交换群,$f:X\to Y$,$\alpha\in X$,$\beta\in Y$,令

$$p_f(\alpha\to\beta)=\frac{1}{|X|}\#\{x\in X:f(x+\alpha)-f(x)=\beta\},$$

则称 $p_f(\alpha\to\beta)$ 为 f 在输入差为 α 的条件下,输出差为 β 的差分概率.此外,也称 $\alpha\to\beta$ 为 f 的一个差分对应,并称 $p_f(\alpha\to\beta)$ 为该差分对应的概率.其中,"$|\cdot|$"和"$\#\{\cdot\}$"都表示集合元素个数.

定义 2[16] 设$(X,+)$是有限交换群,$f_{(k_1,\cdots,k_n)}=f_{k_n}\cdots f_{k_2}f_{k_1}$,$\alpha_1,\cdots,\alpha_{n+1}\in X$,则称 $\alpha_1\to\alpha_2\to\cdots\to\alpha_n\to\alpha_{n+1}$ 为 $f_{(k_1,\cdots,k_n)}$ 的一个起点为 α_1,终点为 α_{n+1} 的差分传递链,并称 $p_{f_{k_1}}(\alpha_1\to\alpha_2)p_{f_{k_2}}(\alpha_2\to\alpha_3)\cdots p_{f_{k_n}}(\alpha_n\to\alpha_{n+1})$ 为该差分传递链的概率.

收稿日期:2015-01-27;**修回日期**:2015-06-10.

基金项目:"十二五"国家密码基金(MMJJ201401007).

第 1 作者简介:殷 勍(1990－),男,河南新乡人,信息工程大学在读硕士研究生,研究方向为密码学.

通信作者简介:王念平(1973－),男,河南洛阳人,信息工程大学副教授,博士,研究方向为密码学,E-mail:wwnnpp@126.com.

在本文中，也称差分传递链 $\alpha_1 \to \alpha_2 \to \cdots \to \alpha_n \to \alpha_{n+1}$ 为 n 轮差分特征.

1.2　模型描述

图 1 所示的是 4 分组扩展广义 Feistel 结构的结构框图，其中 $x_i, y_i, k_j \in Z_2^m (1 \le i \le 4; j = 1,2)$，$(x_1, x_2, x_3, x_4)$ 表示圈函数的输入，(y_1, y_2, y_3, y_4) 表示圈函数的输出，k_j 表示参与轮函数 $f_j: Z_2^m \to Z_2^m$ 的圈子密钥. 由图 1 知，圈函数可记为 $Q_k(x_1, x_2, x_3, x_4) = (x_3 \oplus f_2(x_2 \oplus k_2), x_4 \oplus x_2 \oplus f_1(x_1 \oplus k_1), x_1, x_2)$. 这里需要指出，轮函数 f_1 和 f_2 可以相同，也可以不同，但在以下的讨论中，f_1 和 f_2 是否相同并不影响所得的结论.

针对 4 分组扩展广义 Feistel 结构，引入活动轮函数的定义：

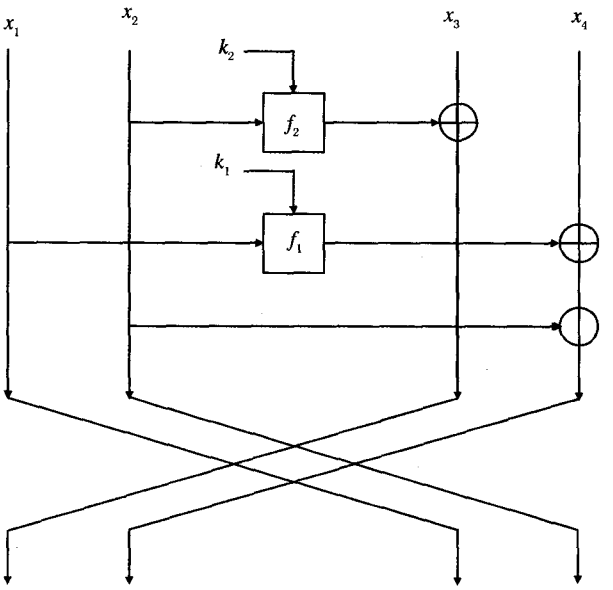

图1 4分组扩展广Feistel结构

定义 3[2]　设 $\alpha \to \beta$ 是轮函数的一个差分对应，若 $\alpha \neq 0$，则此时称该轮函数为(差分) 活动轮函数.

显然，对于 4 分组扩展广义 Feistel 结构，圈函数的差分对应 $(0,0,0,0) \to (0,0,0,0)$ 的概率恒为 1，故称其为平凡差分对应. 本文以下研究的都是非平凡的情况.

2　活动轮函数个数的下界

首先给出差分对应的结构形式.

定理 1　对于 4 分组扩展广义 Feistel 结构，圈函数 $Q_k(x_1, x_2, x_3, x_4) = (x_3 \oplus f_2(x_2 \oplus k_2), x_4 \oplus x_2 \oplus f_1(x_1 \oplus k_1), x_1, x_2)$ 的具有非零概率的差分对应都具有形式 $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \to (\alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1, \alpha_1, \alpha_2)$，且轮函数 f_1 和 f_2 的差分对应分别为 $f_1: \alpha_1 \to \beta_1$，$f_2: \alpha_2 \to \beta_2$，并有

$$p_{Q_k}((\alpha_1, \alpha_2, \alpha_3, \alpha_4) \to (\alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1, \alpha_1, \alpha_2)) = p_{f_1}(\alpha_1 \to \beta_1) \cdot p_{f_2}(\alpha_2 \to \beta_2).$$

证明　令 $\beta_1 = f_1(x_1 \oplus k_1) \oplus f_1(x_1 \oplus \alpha_1 \oplus k_1)$，，则

显然，$Q(x_1, x_2, x_3, x_4) \oplus Q(x_1 \oplus \alpha_1, x_2 \oplus \alpha_2, x_3 \oplus \alpha_3, x_4 \oplus \alpha_4) = (\alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1, \alpha_1, \alpha_2)$ 成立等价于 $\beta_1 = f_1(x_1 \oplus \alpha_1 \oplus k_1) \oplus f_1(x_1 \oplus k_1)$ 和 $\beta_2 = f_2(x_2 \oplus \alpha_2 \oplus k_2) \oplus f_2(x_2 \oplus k_2)$ 同时成立，故 $p_{Q_k}((\alpha_1, \alpha_2, \alpha_3, \alpha_4) \to (\alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1, \alpha_1, \alpha_2)) = p_{f_1}(\alpha_1 \to \beta_1) \cdot p_{f_2}(\alpha_2 \to \beta_2)$.

根据定理 1，可得如下事实：

注 1　$k(k \ge 1)$ 轮差分特征 $(\alpha_1^{(0)}, \alpha_2^{(0)}, \alpha_3^{(0)}, \alpha_4^{(0)}) \to (\alpha_1^{(1)}, \alpha_2^{(1)}, \alpha_3^{(1)}, \alpha_4^{(1)}) \to \cdots \to (\alpha_1^{(k)}, \alpha_2^{(k)}, \alpha_3^{(k)}, \alpha_4^{(k)})$ 中活动轮函数的个数就是集合 $\{\alpha_i^{(j)} \mid i = 1,2; 0 \le j \le k-1\}$ 中非零元素的个数. 显然，活动轮函数的个数与最后一轮输出差分 $(\alpha_1^{(k)}, \alpha_2^{(k)}, \alpha_3^{(k)}, \alpha_4^{(k)})$ 无关.

定理 2　对于 4 分组扩展广义 Feistel 结构，设轮函数都是双射，则 1)1 轮差分特征至少有 0 个活动轮函数；2)2 轮差分特征至少有 1 个活动轮函数；3)3 轮差分特征至少有 2 个活动轮函数；4)4 轮差分特征至少有 3 个活动轮函数；5)5 轮差分特征至少有 4 个活动轮函数.

证明　结论 1) 显然成立，只证结论 2) ～ 5).

由注 1 知，活动轮函数的个数与最后一轮输出差分无关，从而为书写方便起见，将差分特征的最后一轮输出差分记为 $(*, *, *, *)$.

2) 由定理 1，设 2 轮差分特征为 $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \to (\alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1, \alpha_1, \alpha_2) \to (*, *, *, *)$，且第 1 轮的轮函数 $f_1^{(1)}$ 和 $f_2^{(1)}$ 的差分对应分别为 $f_1^{(1)}: \alpha_1 \to \beta_1$，$f_2^{(1)}: \alpha_2 \to \beta_2$，其中 $f_i^{(j)} (i = 1,2)$ 表示第 j 轮的轮函数 f_i(下同). 由“非平凡差分对应”的含义知，$\alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1, \alpha_1, \alpha_2$ 不全为零，即 $\alpha_1, \alpha_2, \alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1$ 不全为零，故由注 1 知，2 轮差分特征至少有 1 个活动轮函数.

3) 由定理 1，设 3 轮差分特征为 $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \to (\alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1, \alpha_1, \alpha_2) \to (\alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3,$

$\alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1) \to (*,*,*,*)$,且第 1、2 轮的轮函数的差分对应分别为 $f_1^{(1)}: \alpha_1 \to \beta_1, f_2^{(1)}: \alpha_2 \to \beta_2$, $f_1^{(2)}: \alpha_3 \oplus \beta_2 \to \beta_3, f_2^{(2)}: \alpha_4 \oplus \alpha_2 \oplus \beta_1 \to \beta_4$.

此时,$\alpha_1, \alpha_2, \alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3$ 不可能全为零. 否则,由 $\alpha_1 = \alpha_1 \oplus \beta_4 = 0$ 知 $\beta_4 = 0$,从而由差分对应 $f_2^{(2)}: \alpha_4 \oplus \alpha_2 \oplus \beta_1 \to \beta_4$、$\beta_4 = 0$ 以及轮函数是双射知 $\alpha_4 \oplus \alpha_2 \oplus \beta_1 = 0$,而由差分对应 $f_1^{(1)}: \alpha_1 \to \beta_1$ 和 $\alpha_1 = 0$ 知 $\beta_1 = 0$,故再由假设 $\alpha_2 = 0$ 知 $\alpha_4 = \alpha_2 \oplus \beta_1 = 0 \oplus 0 = 0$,即 $\alpha_4 = 0$,又由假设知 $\alpha_4 \oplus \beta_1 \oplus \beta_3 = 0$,从而 $\beta_3 = \alpha_4 \oplus \beta_1 = 0 \oplus 0 = 0$,即 $\beta_3 = 0$,进而由差分对应 $f_1^{(2)}: \alpha_3 \oplus \beta_2 \to \beta_3$、$\beta_3 = 0$ 以及轮函数是双射知 $\alpha_3 \oplus \beta_2 = 0$,于是$(\alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3, \alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1) = (0,0,0,0)$,这与"非平凡差分对应"的含义矛盾,故 $\alpha_1, \alpha_2, \alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3$ 不可能全为零,从而可分以下两种情形进行讨论.

情形 A:当 α_1, α_2 不全为零时. 由结论 2) 知,2 轮差分特征$(\alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1, \alpha_1, \alpha_2) \to (\alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3, \alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1) \to (*,*,*,*)$ 至少有 1 个活动轮函数,从而由注 1 知,$\alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1, \alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3$ 至少有 1 个不为零,再由前提条件知 α_1, α_2 不全为零,故 $\alpha_1, \alpha_2, \alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1, \alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3$ 至少有 2 个不为零,进而由注 1 知,3 轮差分特征至少有 2 个活动轮函数.

情形 B:当 $\alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3$ 不全为零时. 由结论 2) 知,2 轮差分特征$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \to (\alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1, \alpha_1, \alpha_2) \to (\alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3, \alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1)$ 至少有 1 个活动轮函数,从而由注 1 知,$\alpha_1, \alpha_2, \alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1$ 至少有 1 个不为零,再由前提条件知 $\alpha_1 \oplus \beta_4$, $\alpha_4 \oplus \beta_1 \oplus \beta_3$ 不全为零,故 $\alpha_1, \alpha_2, \alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1, \alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3$ 至少有 2 个不为零,进而由注 1 知,3 轮差分特征至少有 2 个活动轮函数.

综合情形 A 和情形 B 可知,3 轮差分特征至少有 2 个活动轮函数.

4) 由定理 1,设 4 轮差分特征为$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \to (\alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1, \alpha_1, \alpha_2) \to (\alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3, \alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1) \to (\alpha_3 \oplus \beta_2 \oplus \beta_6, \alpha_2 \oplus \beta_3 \oplus \beta_5, \alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3) \to (*,*,*,*)$,且第 1、2、3 轮的轮函数的差分对应分别为 $f_1^{(1)}: \alpha_1 \to \beta_1, f_2^{(1)}: \alpha_2 \to \beta_2, f_1^{(2)}: \alpha_3 \oplus \beta_2 \to \beta_3, f_2^{(2)}: \alpha_4 \oplus \alpha_2 \oplus \beta_1 \to \beta_4, f_1^{(3)}: \alpha_1 \oplus \beta_4 \to \beta_5, f_2^{(3)}: \alpha_4 \oplus \beta_1 \oplus \beta_3 \to \beta_6$.

以下分 3 种情形进行讨论.

情形 A:当 α_1, α_2 不全为零时. 由结论 3) 知,3 轮差分特征$(\alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1, \alpha_1, \alpha_2) \to (\alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3, \alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1) \to (\alpha_3 \oplus \beta_2 \oplus \beta_6, \alpha_2 \oplus \beta_3 \oplus \beta_5, \alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3) \to (*,*,*,*)$ 至少有 2 个活动轮函数,从而由注 1 知,$\alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1, \alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3, \alpha_3 \oplus \beta_2 \oplus \beta_6, \alpha_2 \oplus \beta_3 \oplus \beta_5$ 至少有 2 个不为零,再由前提条件知 α_1, α_2 不全为零,故 $\alpha_1, \alpha_2, \alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1$, $\alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3, \alpha_3 \oplus \beta_2 \oplus \beta_6, \alpha_2 \oplus \beta_3 \oplus \beta_5$ 至少有 3 个不为零,进而由注 1 知,4 轮差分特征至少有 3 个活动轮函数.

情形 B:当 $\alpha_3 \oplus \beta_2 \oplus \beta_6, \alpha_2 \oplus \beta_3 \oplus \beta_5$ 不全为零时. 由结论(3) 知,3 轮差分特征$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \to (\alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1, \alpha_1, \alpha_2) \to (\alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3, \alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1) \to (\alpha_3 \oplus \beta_2 \oplus \beta_6, \alpha_2 \oplus \beta_3 \oplus \beta_5, \alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3)$ 至少有 2 个活动轮函数,从而由注 1 知,$\alpha_1, \alpha_2, \alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1, \alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3$ 至少有 2 个不为零,再由前提条件知 $\alpha_3 \oplus \beta_2 \oplus \beta_6, \alpha_2 \oplus \beta_3 \oplus \beta_5$ 不全为零,故 $\alpha_1, \alpha_2, \alpha_3 \oplus \beta_2, \alpha_4 \oplus \alpha_2 \oplus \beta_1, \alpha_1 \oplus \beta_4, \alpha_4 \oplus \beta_1 \oplus \beta_3, \alpha_3 \oplus \beta_2 \oplus \beta_6, \alpha_2 \oplus \beta_3 \oplus \beta_5$ 至少有 3 个不为零,进而由注 1 知,4 轮差分特征至少有 3 个活动轮函数.

情形 C:当 $\alpha_1, \alpha_2, \alpha_3 \oplus \beta_2 \oplus \beta_6, \alpha_2 \oplus \beta_3 \oplus \beta_5$ 全为零时. 由轮函数的差分对应 $f_1^{(1)}: \alpha_1 \to \beta_1, f_2^{(1)}: \alpha_2 \to \beta_2$ 和 α_1, α_2 全为零知 $\beta_1 = \beta_2 = 0$,从而由前提条件 $\alpha_3 \oplus \beta_2 \oplus \beta_6 = \alpha_2 \oplus \beta_3 \oplus \beta_5 = 0$ 知 $\beta_6 = \alpha_3 \oplus \beta_2 = \alpha_3, \beta_5 = \alpha_2 \oplus \beta_3 = \beta_3$,即 $\beta_6 = \alpha_3, \beta_5 = \beta_3$,进而第 1、2、3 轮的轮函数的差分对应分别变成 $f_1^{(1)}: 0 \to 0, f_2^{(1)}: 0 \to 0, f_1^{(2)}: \alpha_3 \to \beta_3, f_2^{(2)}: \alpha_4 \to \beta_4, f_1^{(3)}: \beta_4 \to \beta_3, f_2^{(3)}: \alpha_4 \oplus \beta_3 \to \alpha_3$.

由 α_1, α_2 全为零和"非平凡差分对应"的含义知 α_3, α_4 不全为零,由差分对应 $f_1^{(2)}: \alpha_3 \to \beta_3$ 以及轮函数是双射知,α_3 与 β_3 或全为零或全不为零,由差分对应 $f_1^{(3)}: \beta_4 \to \beta_3$ 以及轮函数是双射知,β_4 与 β_3 或全为零或全不为零,由 $f_2^{(2)}: \alpha_4 \to \beta_4$ 以及轮函数是双射知,α_4 与 β_4 或全为零或全不为零,即 $\alpha_3, \alpha_4, \beta_3, \beta_4$ 或全为零或全不为零,再由"非平凡差分对应"的含义知 $\alpha_3 \neq 0, \alpha_4 \neq 0$,故 $\alpha_3 \neq 0, \alpha_4 \neq 0, \beta_4 \neq 0$,这也就是说 $\alpha_3 \oplus \beta_2 = \alpha_3 \neq 0, \alpha_4 \oplus \alpha_2 \oplus \beta_1 = \alpha_4 \neq 0, \alpha_1 \oplus \beta_4 = \beta_4 \neq 0$,即至少有 3 个轮函数的输入差分不为零,故 4 轮差分特征至少有 3 个活动轮函数.

综合情形 A、情形 B 和情形 C 可知,4 轮差分特征至少有 3 个活动轮函数.

5) 由定理 1,设 5 轮差分特征为$(\alpha_1,\alpha_2,\alpha_3,\alpha_4)\to(\alpha_3\oplus\beta_2,\alpha_4\oplus\alpha_2\oplus\beta_1,\alpha_1,\alpha_2)\to(\alpha_1\oplus\beta_4,\alpha_4\oplus\beta_1\oplus\beta_3,\alpha_3\oplus\beta_2,\alpha_4\oplus\alpha_2\oplus\beta_1)\to(\alpha_3\oplus\beta_2\oplus\beta_6,\alpha_2\oplus\beta_3\oplus\beta_5,\alpha_1\oplus\beta_4,\alpha_4\oplus\beta_1\oplus\beta_3)\to(\alpha_1\oplus\beta_4\oplus\beta_8,\alpha_2\oplus\alpha_4\oplus\beta_1\oplus\beta_5\oplus\beta_7,\alpha_3\oplus\beta_2\oplus\beta_6,\alpha_2\oplus\beta_3\oplus\beta_5)\to(*,*,*,*)$,且第 1、2、3、4 轮的轮函数的差分对应分别为 $f_1^{(1)}:\alpha_1\to\beta_1$,$f_2^{(1)}:\alpha_2\to\beta_2$,$f_1^{(2)}:\alpha_3\oplus\beta_2\to\beta_3$,$f_2^{(2)}:\alpha_4\oplus\alpha_2\oplus\beta_1\to\beta_4$,$f_1^{(3)}:\alpha_1\oplus\beta_4\to\beta_5$,$f_2^{(3)}:\alpha_4\oplus\beta_1\oplus\beta_3\to\beta_6$,$f_1^{(4)}:\alpha_3\oplus\beta_2\oplus\beta_6\to\beta_7$,$f_2^{(4)}:\alpha_2\oplus\beta_3\oplus\beta_5\to\beta_8$.

以下分 3 种情形进行讨论.

情形 A:当 α_1,α_2 不全为零时. 由结论 4) 知,4 轮差分特征$(\alpha_3\oplus\beta_2,\alpha_4\oplus\alpha_2\oplus\beta_1,\alpha_1,\alpha_2)\to(\alpha_1\oplus\beta_4,\alpha_4\oplus\beta_1\oplus\beta_3,\alpha_3\oplus\beta_2,\alpha_4\oplus\alpha_2\oplus\beta_1)\to(\alpha_3\oplus\beta_2\oplus\beta_6,\alpha_2\oplus\beta_3\oplus\beta_5,\alpha_1\oplus\beta_4,\alpha_4\oplus\beta_1\oplus\beta_3)\to(\alpha_1\oplus\beta_4\oplus\beta_8,\alpha_2\oplus\alpha_4\oplus\beta_1\oplus\beta_5\oplus\beta_7,\alpha_3\oplus\beta_2\oplus\beta_6,\alpha_2\oplus\beta_3\oplus\beta_5)\to(*,*,*,*)$ 至少有 3 个活动轮函数,从而由注 1 知,$\alpha_3\oplus\beta_2,\alpha_4\oplus\alpha_2\oplus\beta_1,\alpha_1\oplus\beta_4,\alpha_4\oplus\beta_1\oplus\beta_3,\alpha_3\oplus\beta_2\oplus\beta_6,\alpha_2\oplus\beta_3\oplus\beta_5,\alpha_1\oplus\beta_4\oplus\beta_8,\alpha_2\oplus\alpha_4\oplus\beta_1\oplus\beta_5\oplus\beta_7$ 至少有 3 个不为零,再由前提条件知 α_1,α_2 不全为零,故 $\alpha_1,\alpha_2,\alpha_3\oplus\beta_2,\alpha_4\oplus\alpha_2\oplus\beta_1,\alpha_1\oplus\beta_4,\alpha_4\oplus\beta_1\oplus\beta_3,\alpha_3\oplus\beta_2\oplus\beta_6,\alpha_2\oplus\beta_3\oplus\beta_5,\alpha_1\oplus\beta_4\oplus\beta_8,\alpha_2\oplus\alpha_4\oplus\beta_1\oplus\beta_5\oplus\beta_7$ 至少有 4 个不为零,进而由注 1 知,5 轮差分特征至少有 4 个活动轮函数.

情形 B:当 $\alpha_1\oplus\beta_4\oplus\beta_8,\alpha_2\oplus\alpha_4\oplus\beta_1\oplus\beta_5\oplus\beta_7$ 不全为零时. 由结论 4) 知,4 轮差分特征$(\alpha_1,\alpha_2,\alpha_3,\alpha_4)\to(\alpha_3\oplus\beta_2,\alpha_4\oplus\alpha_2\oplus\beta_1,\alpha_1,\alpha_2)\to(\alpha_1\oplus\beta_4,\alpha_4\oplus\beta_1\oplus\beta_3,\alpha_3\oplus\beta_2,\alpha_4\oplus\alpha_2\oplus\beta_1)\to(\alpha_3\oplus\beta_2\oplus\beta_6,\alpha_2\oplus\beta_3\oplus\beta_5,\alpha_1\oplus\beta_4,\alpha_4\oplus\beta_1\oplus\beta_3)\to(\alpha_1\oplus\beta_4\oplus\beta_8,\alpha_2\oplus\alpha_4\oplus\beta_1\oplus\beta_5\oplus\beta_7,\alpha_3\oplus\beta_2\oplus\beta_6,\alpha_2\oplus\beta_3\oplus\beta_5)$ 至少有 3 个活动轮函数,从而由注 1 知,$\alpha_1,\alpha_2,\alpha_3\oplus\beta_2,\alpha_4\oplus\alpha_2\oplus\beta_1,\alpha_1\oplus\beta_4,\alpha_4\oplus\beta_1\oplus\beta_3,\alpha_3\oplus\beta_2\oplus\beta_6,\alpha_2\oplus\beta_3\oplus\beta_5$ 至少有 3 个不为零,再由前提条件知 $\alpha_1\oplus\beta_4\oplus\beta_8,\alpha_2\oplus\alpha_4\oplus\beta_1\oplus\beta_5\oplus\beta_7$ 不全为零,故 $\alpha_1,\alpha_2,\alpha_3\oplus\beta_2,\alpha_4\oplus\alpha_2\oplus\beta_1,\alpha_1\oplus\beta_4,\alpha_4\oplus\beta_1\oplus\beta_3,\alpha_3\oplus\beta_2\oplus\beta_6,\alpha_2\oplus\beta_3\oplus\beta_5,\alpha_1\oplus\beta_4\oplus\beta_8,\alpha_2\oplus\alpha_4\oplus\beta_1\oplus\beta_5\oplus\beta_7$ 至少有 4 个不为零,进而由注 1 知,5 轮差分特征至少有 4 个活动轮函数.

情形 C:当 $\alpha_1,\alpha_2,\alpha_1\oplus\beta_4\oplus\beta_8,\alpha_2\oplus\alpha_4\oplus\beta_1\oplus\beta_5\oplus\beta_7$ 全为零时. 由轮函数的差分对应 $f_1^{(1)}:\alpha_1\to\beta_1$,$f_2^{(1)}:\alpha_2\to\beta_2$ 和 α_1,α_2 全为零知 $\beta_1=\beta_2=0$,由 $\alpha_1\oplus\beta_4\oplus\beta_8,\alpha_2\oplus\alpha_4\oplus\beta_1\oplus\beta_5\oplus\beta_7$ 全为零知 $\beta_8=\alpha_1\oplus\beta_4,\beta_7=\alpha_2\oplus\alpha_4\oplus\beta_1\oplus\beta_5$,从而再由前提条件 $\alpha_1=\alpha_2=0$ 知 $\beta_8=\beta_4,\beta_7=\alpha_4\oplus\beta_5$,进而第 1、2、3、4 轮的轮函数的差分对应分别变成 $f_1^{(1)}:0\to0$,$f_2^{(1)}:0\to0$,$f_1^{(2)}:\alpha_3\to\beta_3$,$f_2^{(2)}:\alpha_4\to\beta_4$,$f_1^{(3)}:\beta_4\to\beta_5$,$f_2^{(3)}:\alpha_4\oplus\beta_3\to\beta_6$,$f_1^{(4)}:\alpha_3\oplus\beta_6\to\alpha_4\oplus\beta_5$,$f_2^{(4)}:\beta_3\oplus\beta_5\to\beta_4$.

由 α_1,α_2 全为零和"非平凡差分对应"的含义知 α_3,α_4 不全为零.

下面首先证 $\alpha_4\neq0$.(反证法)

若 $\alpha_4=0$,则由轮函数的差分对应 $f_2^{(2)}:\alpha_4\to\beta_4$,$f_2^{(4)}:\beta_3\oplus\beta_5\to\beta_4$ 以及轮函数是双射知 $\alpha_4=\beta_4=\beta_3\oplus\beta_5=0$,从而由 $\beta_4=0$ 和轮函数的差分对应 $f_1^{(3)}:\beta_4\to\beta_5$ 知 $\beta_5=0$,进而由 $\beta_3\oplus\beta_5=0$ 知 $\beta_3=\beta_5=0$. 于是,由 $\beta_3=0$ 和轮函数的差分对应 $f_1^{(2)}:\alpha_3\to\beta_3$ 以及轮函数是双射知 $\alpha_3=0$,再由假设条件知 $\alpha_3=\alpha_4=0$,这与 α_3,α_4 不全为零矛盾,故 $\alpha_4\neq0$.

因为 $\alpha_4\neq0$,故由轮函数的差分对应 $f_2^{(2)}:\alpha_4\to\beta_4$,$f_2^{(4)}:\beta_3\oplus\beta_5\to\beta_4$ 知 $\beta_4\neq0,\beta_3\oplus\beta_5\neq0$,再由轮函数的差分对应 $f_2^{(3)}:\alpha_4\oplus\beta_3\to\beta_6$ 和 $\alpha_4\neq0$ 知 β_3,β_6 不全为零(否则将有 $f_2^{(3)}:\alpha_4\to0$,这与轮函数是双射矛盾),从而由轮函数的差分对应 $f_1^{(2)}:\alpha_3\to\beta_3$,$f_2^{(3)}:\alpha_4\oplus\beta_3\to\beta_6$ 知 $\alpha_3,\alpha_4\oplus\beta_3$ 不全为零,也就是说,$\alpha_4\neq0,\beta_4\neq0,\beta_3\oplus\beta_5\neq0$ 且 $\alpha_3,\alpha_4\oplus\beta_3$ 不全为零,即至少有 4 个轮函数的输入差分不为零,故 5 轮差分特征至少有 4 个活动轮函数.

综合情形 A、情形 B 和情形 C 可知,5 轮差分特征至少有 4 个活动轮函数.

由(1) ~ (5) 知,本定理结论成立.

由定理 2 立得如下结论.

定理 3　对于 4 分组扩展广义 Feistel 结构,设轮函数都是双射,则 $r=5k+t(k\geq0,0\leq t\leq4)$ 轮差分特征至少有 $4k+\lambda(t)$ 个活动轮函数,其中 $\lambda(t)=\begin{cases}t-1,1\leq t\leq4,\\0,t=0.\end{cases}$

证明　将任意 $r=5k+t(k\geq0,0\leq t\leq4)$ 轮差分特征按顺序拆分成 k 个 5 轮差分特征和一个 t 轮差分特征,由定理 2 知,5 轮差分特征至少有 4 个活动轮函数,从而 k 个 5 轮差分特征至少有 $4k$ 个活动轮函数,

同时由定理 2 知,$t(1 \leq t \leq 4)$ 轮差分特征至少有 $t-1$ 个活动轮函数,故 $r=5k+t(k \geq 0, 0 \leq t \leq 4)$ 轮差分特征至少有 $4k+\lambda(t)$ 个活动轮函数,所以定理 3 结论成立.

例如,6 轮差分特征可以拆分成一个 5 轮差分特征和一个 1 轮差分特征,由定理 2 知,5 轮差分特征至少有 4 个活动轮函数,1 轮差分特征至少有 0 个活动轮函数,故 6 轮差分特征至少有 4 个活动轮函数.

定理 4 对于 4 分组扩展广义 Feistel 结构,设轮函数都是双射,且令 p 表示轮函数的最大差分概率,则 $r=5k+t(k \geq 0, 0 \leq t \leq 4)$ 轮差分特征概率的上界为 $p^{4k+\lambda(t)}$,其中 $\lambda(t)=\begin{cases} t-1, 1 \leq t \leq 4, \\ 0, t=0. \end{cases}$

3 结束语

本文对 4 分组扩展广义 Feistel 结构抵抗差分密码分析的能力进行了详细的研究. 在轮函数为双射的假设条件下,给出了任意轮差分特征中活动轮函数个数的下界. 本文结果的意义在于:采用该类扩展广义 Feistel 结构设计分组密码时,只要使得相应轮函数的最大差分概率 p 足够小,就能估计并保证整个算法抵抗差分密码分析的能力. 进一步要做的工作是讨论该类密码抵抗其他密码分析方法的能力.

参 考 文 献

[1] Nyberg K. Generalized Feistel networks[C]. Advances in Cryptology-ASIACRYPT' 96, Kyongju, 1996.

[2] Schneier B, Kelsey J. Unbalanced Feistel networks and block cipher design[C]. Fast Software Encryption'95, Cambridge, 1995.

[3] 吴文玲,贺也平. 一类广义 Feistel 密码的安全性评估[J]. 电子与信息学报,2002,24(9):1177-1184.

[4] Wang Q Y, Zhang B. Practical security against differential and linear cryptanalysis for SMS4-like Cipher[J]. Journal of Networks, 2013, 8(8):1689-1693.

[5] 王念平. 一类广义 Feistel 密码的安全性能分析[J]. 大连海事大学学报,2007,33(3):63-67.

[6] Shirai T, Araki K. On generalized Feistel structures using the diffusion switching mechanism[J]. IEICE T FUND ELECTR, 2008, 91(8):2120-2129.

[7] Adams C. The CAST-256 Encryption Algorithm[J]. Computer Science & Communications Dictionary, 2001, 81(4):864-894.

[8] Rivest R, Robshaw M. The RC6 block cipher[EB/OL]. [2015-01-03]. http://cs. usu. edu. ru/crypto/RC6/rc6v11. pdf.

[9] Shirai T, Shibutani K. The 128-bit block cipher CLEFIA[C]. Fast Software Encryption'07, Luxembourg, 2007.

[10] Burwick C, Coppersmith D. MARS-a candidate cipher for AES[EB/OL]. [2015-01-10]. http://cryptosoft. de/docs/Mars. pdf.

[11] Suzaki T, Minematsu K. Improving the generalized Feistel[C]. Fast Software Encryption'10, Seoul, 2010.

[12] Yanagihara S, Iwata T. Improving the permutation layer of Type 1, Type 3, Source-Heavy, and Target-Heavy generalized feistel structures[J]. IEICE T FUND ELECTR, 2013, 96(1):2-14.

[13] Berger T P, Minier M. Extended generalized Feistel networks using matrix representation[C]. SAC 2013, Burnaby, 2013.

[14] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems[J]. Journal of CRYPTOLOGY, 1991, 4(1):3-72.

[15] Knudsen L R. Practically secure Feistel ciphers[C]. Fast Software Encryption'93, Cambridge, 1993.

[16] 金晨辉,郑浩然. 密码学[M]. 北京:高等教育出版社,2009:175-186.

Lower Bounds on the Number of Active Round Functions for a Class of Extended Generalized Feistel Structure

YIN Qing, WANG Nianping

(School of Cryptography Engineering, PLA Information Engineering University, Zhengzhou 450000, China)

Abstract: Extended generalized Feistel structure has been proposed recently as a building structure of block cipher. To evaluate the security of this structure, the security analysis of four-block extended generalized Feistel structure against differential and linear cryptanalysis is investigated in detail. Lower bounds on the number of active round functions for arbitrary round differential characteristics is given when round functions are all bijective.

Keywords: extended generalized Feistel structure; differential cryptanalysis; active round function; lower bounds