一类广义 Feistel 密码的安全性评估 [1]

吴文玲 贺也平

(中国科学院软件研究所信息安全国家重点实验室 北京 100080)
(中国科学院信息安全技术工程研究中心 北京 100080)

摘 要 该文评估一类广义 Feistel 密码 (GFC) 抵抗差分和线性密码分析的能力：如果轮函数是双射且它的最大差分和线性特征的概率分别是 p 和 q，则 16 轮 GFC 的差分和线性特征的概率的上界为 p^7 和 q^7；如果轮函数采用 SP 结构且是双射，S 盒的最大差分和线性特征的概率是 p_S 和 q_S，P 变换的分支数为 P_d，则 16 轮 GFC 的差分和线性特征的概率的上界为 $(p_S)^{3P_d+1}$ 和 $(q_S)^{3P_d+1}$.

关键词 差分密码分析，线性密码分析，分支数，密码，S 盒
中图号 TN918.1

1 引 言

差分密码分析 [1] 和线性密码分析 [2] 是目前已知的最有效的理论攻击方法，因此，每个分组密码设计者都要想办法估计新算法抵抗差分密码分析和线性密码分析的能力。现有的做法是给出最大差分和线性特征的概率或给出差分和线性特征的概率的上界。对目前流行的 Feistel 密码 (以 DES 为代表) 和 SP 密码 (以 Square 为代表)，有大量文献讨论此问题。针对 SP 密码，文献 [3] 介绍了分支数的概念，分支数代表了连续两轮非平凡差分 (线性) 特征中活动 S-盒的最小数目。因为每个活动 S-盒都降低了差分 (线性) 特征的概率，所以分支数给出了连续两轮差分 (线性) 特征概率的上界。针对 Feistel 密码，文献 [4] 给出如下结果：

结果 1 对于具有独立子密钥的 r-轮 Feistel 密码，令 p 和 q 分别表示轮函数的最大差分和线性特征概率，$\mathrm{DCP}^r_{\max}$ 和 $\mathrm{LCQ}^r_{\max}$ 分别表示 r-轮最大差分和线性特征概率；则有

(1) 当 $r=2m, 2m+1$ 时，$\mathrm{DCP}^r_{\max} \le p^m$, $\mathrm{LCQ}^r_{\max} \le q^m$;

(2) 当 $r=3m, 3m+1$, 且轮函数是双射时，$\mathrm{DCP}^r_{\max} \le p^{2m}$, $\mathrm{LCQ}^r_{\max} \le q^{2m}$;

(3) 当 $r=3m+2$, 且轮函数是双射时，$\mathrm{DCP}^r_{\max} \le p^{2m+1}$, $\mathrm{LCQ}^r_{\max} \le q^{2m+1}$.

文献 [5] 进一步讨论了轮函数使用 SP 结构的 Feistel 密码的情况，给出了下面的结果：

结果 2 对于具有独立子密钥的 4r-轮 Feistel 密码，如果轮函数采用 SP 结构，且 S 和 P 都是双射，则差分和线性活动的盒子数都不小于 $r \times P_d + \lfloor r/2 \rfloor$. 其中活动盒子和 P_d 如下定义：

定义 1 差分活动 S-盒是指输入差分非 0 的 S-盒；线性活动 S-盒是指输出的表示向量非 0 的 S-盒.

定义 2 令 $P:(F_2^m)^n \to (F_2^m)^n$, $X \to P(X)=Y$, P 的分支数 P_d 定义如下：

$$P_d = \min_{\Delta X \neq 0}(H_w(\Delta X) + H_w(\Delta Y))$$

其中 $X=(x_1,\cdots,x_n) \in (F_2^m)^n$, $x_i \in F_2^m$, ΔX 表示 X 的差分向量，$H_w(\Delta X)$ 是 ΔX 的表示向量的汉明重量.

C.Adams 在文献 [6] 中推出了如图 1 所示的广义 Feistel 密码 (GFC)，此结构的最大优点是：能够直接重用过去的轮函数。众所周知，过去的分组密码都是 64bit 分组长度，而随着计算

[1] 2000-10-08 收到，2001-05-08 定稿
973 项目 (No.G1999035802) 和国家自然科学基金 (No.60103023) 资助

能力的提高，现在设计分组密码都要求是 128bit 分组长度；对于传统 Feistel 密码，分组长度的增加意味着轮函数规模的增加，而构造大规模的轮函数又是比较困难的；如图 1 所示的广义 Feistel 结构为我们设计密码创造了一条捷径．因此，本文我们讨论此结构抵抗差分和线性密码分析的能力．

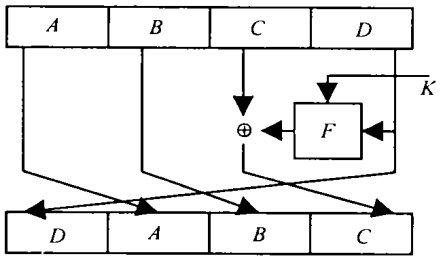

图 1 1 轮 GFC

2 估计 16 轮 GFC 抵抗差分和线性攻击的能力

假定轮函数都是双射，我们用 $(x_{4i+3}, x_{4i+2}, x_{4i+1}, x_{4i})$, $(\Delta x_{4i+3}, \Delta x_{4i+2}, \Delta x_{4i+1}, \Delta x_{4i})$ $(0 \le i \le 15)$ 表示第 $i+1$ 轮的输入和输入差分．为了方便，我们不考虑具体的差分，用 " 1 " 表示不为 0 的差分；因此，输入非 0 差分仅有 15 种表示： $1 = (0\,0\,0\,1), \cdots, 15 = (1\,1\,1\,1)$ ．

2.1 4 轮 GFC

$$1 = (0\,0\,0\,1) \to (1\,0\,0\,1) \to (1\,1\,0\,1) \to (1\,1\,1\,1) \to \begin{cases} (1111) = 15 \\ (1110) = 14 \end{cases}$$

因为轮函数是双射，所以输入非 0 差分，则输出差分一定非 0 ．因此前 3 轮比较清楚．对于第 4 轮，当 Δx_{12} 和 Δx_{13} 都不为 0 时， $F(\Delta x_{12})$ 和 Δx_{13} 有可能相等，因此，输出有两种情况．而且每一轮的输入差分都非 0 ，即 Δx_0, Δx_4, Δx_8 和 Δx_{12} 都不为 0 ．我们用下列记号表示输入为 $1 = (0\,0\,0\,1)$ 的 4 轮 GFC ：

$$1 \begin{cases} \xrightarrow{4(4)} 14 & \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \\ \xrightarrow{4(4)} 15 & \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \end{cases}$$

类似地，我们给出输入为其它值的情况：

$$2 \xrightarrow{4(4)} 15 \quad \Delta x_4 \Delta x_8 \Delta x_{12}$$

$$3 \begin{cases} \xrightarrow{4(1)} 1 & \Delta x_0 \\ \xrightarrow{4(4)} 14 & \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \\ \xrightarrow{4(4)} 15 & \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \end{cases}$$

$$6 \begin{cases} \xrightarrow{4(1)} 2 & \Delta x_4 \\ \xrightarrow{4(3)} 15 & \Delta_4 \Delta x_8 \Delta x_{12} \end{cases}$$

$$4 \xrightarrow{4(2)} 13 \quad \Delta x_8 \Delta x_{12}$$

$$5 \begin{cases} \xrightarrow{4(2)} 3 & \Delta x_0 \Delta x_4 \\ \xrightarrow{4(4)} 14 & \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \\ \xrightarrow{4(4)} 15 & \Delta x_0 \Delta x_4 \Delta x_8 \Delta x_{12} \end{cases}$$

$$8 \xrightarrow{4(1)} 9 \quad \Delta x_{12}$$

$$
\begin{array}{l}
7\left\{\begin{array}{ll}
\xrightarrow{4(2)}3 & \Delta x_0\Delta x_4\\
\xrightarrow{4(3)}12 & \Delta x_0\Delta x_8\Delta x_{12}\\
\xrightarrow{4(3)}13 & \Delta x_0\Delta x_8\Delta x_{12}\\
\xrightarrow{4(4)}14 & \Delta x_0\Delta x_4\Delta x_8\Delta x_{12}\\
\xrightarrow{4(4)}15 & \Delta x_0\Delta x_4\Delta x_8\Delta x_{12}
\end{array}\right.\\
10\left\{\begin{array}{ll}
\xrightarrow{4(2)}6 & \Delta x_4\Delta x_8\\
\xrightarrow{4(3)}15 & \Delta x_4\Delta x_8\Delta x_{12}
\end{array}\right.\\
13\left\{\begin{array}{ll}
\xrightarrow{4(2)}5 & \Delta x_0\Delta x_8\\
\xrightarrow{4(3)}12 & \Delta x_0\Delta x_8\Delta x_{12}\\
\xrightarrow{4(3)}13 & \Delta x_0\Delta x_8\Delta x_{12}
\end{array}\right.\\
15\left\{\begin{array}{ll}
\xrightarrow{4(2)}5 & \Delta x_0\Delta x_8\\
\xrightarrow{4(3)}7 & \Delta x_0\Delta x_4\Delta x_8\\
\xrightarrow{4(3)}10 & \Delta x_0\Delta x_4\Delta x_{12}\\
\xrightarrow{4(3)}11 & \Delta x_0\Delta x_4\Delta x_{12}\\
\xrightarrow{4(3)}12 & \Delta x_0\Delta x_8\Delta x_{12}\\
\xrightarrow{4(3)}13 & \Delta x_0\Delta x_8\Delta x_{12}\\
\xrightarrow{4(4)}14 & \Delta x_0\Delta x_4\Delta x_8\Delta x_{12}\\
\xrightarrow{4(4)}15 & \Delta x_0\Delta x_4\Delta x_8\Delta x_{12}
\end{array}\right.
\end{array}
\qquad
\begin{array}{l}
9\left\{\begin{array}{ll}
\xrightarrow{4(3)}7 & \Delta x_0\Delta x_4\Delta x_8\\
\xrightarrow{4(4)}14 & \Delta x_0\Delta x_4\Delta x_8\Delta x_{12}\\
\xrightarrow{4(4)}15 & \Delta x_0\Delta x_4\Delta x_8\Delta x_{12}
\end{array}\right.\\
11\left\{\begin{array}{ll}
\xrightarrow{4(3)}7 & \Delta x_0\Delta x_4\Delta x_8\\
\xrightarrow{4(2)}8 & \Delta x_0\,\Delta x_{12}\\
\xrightarrow{4(2)}9 & \Delta x_0\,\Delta x_{12}\\
\xrightarrow{4(4)}14 & \Delta x_0\Delta x_4\Delta x_8\Delta x_{12}\\
\xrightarrow{4(4)}15 & \Delta x_0\Delta x_4\Delta x_8\Delta x_{12}
\end{array}\right.\\
12\left\{\begin{array}{ll}
\xrightarrow{4(1)}4 & \Delta x_8\\
\xrightarrow{4(2)}13 & \Delta x_8\Delta x_{12}
\end{array}\right.\\
14\left\{\begin{array}{ll}
\xrightarrow{4(2)}6 & \Delta x_4\Delta x_8\\
\xrightarrow{4(2)}11 & \Delta x_4\Delta x_{12}\\
\xrightarrow{4(3)}15 & \Delta x_4\Delta x_8\Delta x_{12}
\end{array}\right.
\end{array}
$$

2.2 8 轮 GFC

$$
1\left\{\begin{array}{ll}
\xrightarrow{4(4)}14\left\{\begin{array}{ll}
\xrightarrow{4(2)}6 & \Delta x_0\Delta x_4\Delta x_8\Delta x_{12}\Delta x_{20}\Delta x_{24}\\
\xrightarrow{4(2)}11 & \Delta x_0\Delta x_4\Delta x_8\Delta x_{12}\Delta x_{20}\Delta x_{28}\\
\xrightarrow{4(3)}15 & \Delta x_0\Delta x_4\Delta x_8\Delta x_{12}\Delta x_{20}\Delta x_{24}\Delta x_{28}
\end{array}\right.\\
\xrightarrow{4(4)}15\left\{\begin{array}{ll}
\xrightarrow{4(2)}5 & \Delta x_0\Delta x_4\Delta x_8\Delta x_{12}\Delta x_{16}\Delta x_{24}\\
\xrightarrow{4(3)}7 & \Delta x_0\Delta x_4\Delta x_8\Delta x_{12}\Delta x_{16}\Delta x_{20}\Delta x_{24}\\
\xrightarrow{4(3)}11(10) & \Delta x_0\Delta x_4\Delta x_8\Delta x_{12}\Delta x_{16}\Delta x_{20}\Delta x_{24}\\
\xrightarrow{4(3)}13(12) & \Delta x_0\Delta x_4\Delta x_8\Delta x_{12}\Delta x_{16}\Delta x_{24}\Delta x_{28}\\
\xrightarrow{4(4)}15(14) & \Delta x_0\Delta x_4\Delta x_8\Delta x_{12}\Delta x_{16}\Delta x_{20}\Delta x_{24}\Delta x_{28}
\end{array}\right.
\end{array}\right.
$$

可以看出以 1 = (0 0 0 1) 为输入差分的 8 轮 GFC 至少有 6 个轮函数的输入差分非 0；记为 $N_1(F) \geq 6$。如果轮函数采用 SP 结构，P_d 是 P 的分支数，我们可以证明以 1 = (0 0 0 1) 为输入差分的 8 轮 GFC 至少有 $2P_d + 1$ 个活动盒子：记为 $N_1(S) \geq 2P_d + 1$。

我们以 $1 \xrightarrow{4(4)} 14 \xrightarrow{4(2)} 6$ 为例证明之。

首先需指出：如果 $\Delta Y = \Delta X \oplus \Delta Z$，则 $H_W(\Delta Y) \leq H_W(\Delta X) + H_W(\Delta Z)$。令 $\Delta y_i = F(x) \oplus F(x \oplus \Delta x_i)$，从 8 轮 GFC 的结构知：$\Delta y_{12} = \Delta x_0 \oplus \Delta x_{16}$, $\Delta y_{16} = \Delta x_4 \oplus \Delta x_{20}$, $\Delta y_{20} = \Delta x_8 \oplus \Delta x_{24}$, $\Delta y_{24} = \Delta x_{12} \oplus \Delta x_{28}$。又从分支数 P_d 的定义可知：$H(\Delta y_i) + H(\Delta x_i) \geq P_d$。因此，我们有：$H_W(\Delta x_0) + H_W(\Delta x_{12}) + H_W(\Delta x_{16}) \geq P_d$, $H_W(\Delta x_4) + H_W(\Delta x_{16}) + H_W(\Delta x_{20}) \geq P_d$, $H_W(\Delta x_8) + H_W(\Delta x_{20}) + H_W(\Delta x_{24}) \geq P_d$, $H_W(\Delta x_{12}) + H_W(\Delta x_{24}) + H_W(\Delta x_{28}) \geq P_d$。

对 $1 \xrightarrow{4(4)} 14 \xrightarrow{4(2)} 6$，

$$\begin{aligned} N_1(S) &= H_W(\Delta x_0) + H_W(\Delta x_4) + H_W(\Delta x_8) + H_W(\Delta x_{12}) + H_W(\Delta x_{20}) + H_W(\Delta x_{24}) \\ &\geq H_W(\Delta x_4) + H_W(\Delta y_{12}) + H_W(\Delta x_{12}) + H_W(\Delta y_{20}) + H_W(\Delta x_{20}) \geq 2P_d + 1 \end{aligned}$$

同理可证以 $N_2(F) \geq 5$, $N_2(S) \geq 2P_d + 1$; $N_3(F) \geq 5$, $N_3(S) \geq 2P_d + 1$; $N_4(F) \geq 4$, $N_4(S) \geq 2P_d + 1$; $N_8(F) \geq 4$, $N_8(S) \geq 2P_d$；输入差分为其它值的情况如下：

$$5\begin{cases} N_5(F)=3 & N_5(S)\geq P_d+1 & 5\xrightarrow{4(2)}3\xrightarrow{4(1)}1 & \Delta x_0\Delta x_4\Delta x_{16} \\ N_5(F)\geq 6 & N_5(S)\geq 2P_d+1 & \text{else} & \end{cases}$$

$$6\begin{cases} N_6(F)=4 & N_6(S)\geq P_d+2 & 6\xrightarrow{4(1)}2\xrightarrow{4(3)}15 & \Delta x_4\Delta x_{20}\Delta x_{24}\Delta x_{28} \\ N_6(F)\geq 5 & N_6(S)\geq 2P_d+1 & \text{else} & \end{cases}$$

$$7\begin{cases} N_7(F)=3 & N_7(S)\geq P_d+1 & 7\xrightarrow{4(2)}3\xrightarrow{4(1)}1 & \Delta x_0\Delta x_4\Delta x_{16} \\ N_7(F)=4 & N_7(S)\geq P_d+2 & 7\xrightarrow{4(3)}12\xrightarrow{4(1)}4 & \Delta x_0\Delta x_8\Delta x_{12}\Delta x_{24} \\ N_7(F)=5 & N_7(S)\geq P_d+3 & 7\xrightarrow{4(3)}12\xrightarrow{4(2)}13 & \Delta x_0\Delta x_8\Delta x_{12}\Delta x_{24}\Delta x_{28} \\ N_7(F)\geq 5 & N_7(S)\geq 2P_d+1 & \text{else} & \end{cases}$$

$$9\begin{cases} N_9(F)=5 & N_9(S)\geq P_d+3 & 9\xrightarrow{4(3)}7\xrightarrow{4(2)}3 & \Delta x_0\Delta x_4\Delta x_8\Delta x_{16}\Delta x_{20} \\ N_9(F)\geq 6 & N_9(S)\geq 2P_d+1 & \text{else} & \end{cases}$$

$$
10\begin{cases}
N_{10}(F)=5 & N_{10}(S)\geq P_d+3 & 10\xrightarrow{4(2)}6\xrightarrow{4(3)}15 & \Delta x_4\Delta x_8\Delta x_{20}\Delta x_{24}\Delta x_{28}\\
N_{10}(F)=3 & N_{10}(S)\geq P_d+1 & 10\xrightarrow{4(2)}6\xrightarrow{4(1)}2 & \Delta x_4\Delta x_8\Delta x_{20}\\
N_{10}(F)\geq 5 & N_{10}(S)\geq 2P_d+1 & \text{else} &
\end{cases}
$$

$$
11\begin{cases}
N_{11}(F)=5 & N_{11}(S)\geq P_d+3 & 11\xrightarrow{4(3)}7\xrightarrow{4(2)}3 & \Delta x_0\Delta x_4\Delta x_8\Delta x_{16}\Delta x_{20}\\
N_{11}(F)=3 & N_{11}(S)\geq P_d+1 & 11\xrightarrow{4(2)}8\xrightarrow{4(1)}9 & \Delta x_0\Delta x_{12}\Delta x_{28}\\
N_{11}(F)\geq 5 & N_{11}(S)\geq 2P_d+1 & \text{else} &
\end{cases}
$$

$$
12\begin{cases}
N_{12}(F)=4 & N_{12}(S)\geq P_d+2 & 12\xrightarrow{4(1)}4\xrightarrow{4(3)}15 & \Delta x_8\Delta x_{20}\Delta x_{24}\Delta x_{28}\\
N_{12}(F)\geq 4 & N_{12}(S)\geq 2P_d+1 & \text{else} &
\end{cases}
$$

$$
13\begin{cases}
N_{13}(F)=4 & N_{13}(S)\geq P_d+2 & 13\xrightarrow{4(2)}5\xrightarrow{4(2)}3 & \Delta x_0\Delta x_8\Delta x_{16}\Delta x_{20}\\
N_{13}(F)=4 & N_{13}(S)\geq P_d+2 & 13\xrightarrow{4(3)}12\xrightarrow{4(1)}4 & \Delta x_0\Delta x_8\Delta x_{12}\Delta x_{24}\\
N_{13}(F)=5 & N_{13}(S)\geq P_d+3 & 13\xrightarrow{4(3)}12\xrightarrow{4(2)}13 & \Delta x_0\Delta x_8\Delta x_{12}\Delta x_{24}\Delta x_{28}\\
N_{13}(F)\geq 5 & N_{13}(S)\geq 2P_d+1 & \text{else} &
\end{cases}
$$

$$
14\begin{cases}
N_{14}(F)=5 & N_{14}(S)\geq P_d+3 & 14\xrightarrow{4(2)}6\xrightarrow{4(3)}15 & \Delta x_4\Delta x_8\Delta x_{20}\Delta x_{24}\Delta x_{28}\\
N_{14}(F)=3 & N_{14}(S)\geq P_d+1 & 14\xrightarrow{4(2)}6\xrightarrow{4(1)}2 & \Delta x_4\Delta x_8\Delta x_{20}\\
N_{14}(F)=4 & N_{14}(S)\geq P_d+2 & 14\xrightarrow{4(2)}11\xrightarrow{4(2)}8(9) & \Delta x_4\Delta x_{12}\Delta x_{16}\Delta x_{28}\\
N_{14}(F)\geq 5 & N_{14}(S)\geq 2P_d+1 & \text{else} &
\end{cases}
$$

$$
15\begin{cases}
N_{15}(F)=4 & N_{15}(S)\geq P_d+2 & 15\xrightarrow{4(2)}5\xrightarrow{4(2)}3 & \Delta x_0\Delta x_8\Delta x_{16}\Delta x_{20}\\
N_{15}(F)=5 & N_{15}(S)\geq P_d+2 & 15\xrightarrow{4(3)}7\xrightarrow{4(2)}3 & \Delta x_0\Delta x_4\Delta x_8\Delta x_{16}\Delta x_{20}\\
N_{15}(F)=5 & N_{15}(S)\geq P_d+3 & 15\xrightarrow{4(3)}11\xrightarrow{4(2)}8(9) & \Delta x_0\Delta x_4\Delta x_{12}\Delta x_{16}\Delta x_{28}\\
N_{15}(F)=4 & N_{15}(S)\geq P_d+2 & 15\xrightarrow{4(3)}12\xrightarrow{4(1)}4 & \Delta x_0\Delta x_8\Delta x_{12}\Delta x_{24}\\
N_{15}(F)=5 & N_{15}(S)\geq P_d+3 & 15\xrightarrow{4(3)}12\xrightarrow{4(2)}13 & \Delta x_0\Delta x_8\Delta x_{12}\Delta x_{24}\Delta x_{28}\\
N_{15}(F)\geq 5 & N_{15}(S)\geq 2P_d+1 & \text{else} &
\end{cases}
$$

由以上讨论可得以下引理：

引理 1　对于 8 轮的 GFC ，如果轮函数是双射，则有

(1) 至少有 3 个轮函数的输入差分非 0；

(2) 如果轮函数采用 SP 结构，至少有 P_d+1 个活动盒子，P_d 是 P 的分支数.

2.3 16 轮 GFC

引理 2　对于 16 轮的 GFC，如果轮函数是双射，则有

(1) 至少有 7 个轮函数的输入差分非 0；

(2) 如果轮函数采用 SP 结构，至少有 $3P_d+1$ 个活动盒子，P_d 是 P 的分支数.

证明　(1) 我们只需看 $N_i(F)=3$ 的情况：

$5\xrightarrow{4(2)}3\xrightarrow{4(1)}1$, $7\xrightarrow{4(2)}3\xrightarrow{4(1)}1$, $10\xrightarrow{4(2)}6\xrightarrow{4(1)}2$, $11\xrightarrow{4(2)}8\xrightarrow{4(1)}9$, $14\xrightarrow{4(2)}6\xrightarrow{4(1)}2$. 因为 $N_1(F)\geq 6$, $N_2(F)\geq 5$, $N_9(F)\geq 4$ ，所以 16 轮的 GFC 至少有 7 个轮函数的输入差分非 0 .

证毕

(2) 我们首先列出满足 $N_i(S) \geq P_d + 1$ 的 8 轮 GFC：

$5 \xrightarrow{4(2)} 3 \xrightarrow{4(1)} 1$，$6 \xrightarrow{4(1)} 2 \xrightarrow{4(3)} 15$，$7 \xrightarrow{4(2)} 3 \xrightarrow{4(1)} 1$，
$7 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4$，$7 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13$，$9 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3$
$10 \xrightarrow{4(2)} 6 \xrightarrow{4(1)} 2$，$10 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15$，$11 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3$
$11 \xrightarrow{4(2)} 8 \xrightarrow{4(1)} 9$，$12 \xrightarrow{4(1)} 4 \xrightarrow{4(3)} 15$，$13 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3$
$13 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4$，$13 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13$，$14 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15$
$14 \xrightarrow{4(2)} 6 \xrightarrow{4(1)} 2$，$14 \xrightarrow{4(2)} 11 \xrightarrow{4(2)} 8$，$14 \xrightarrow{4(2)} 11 \xrightarrow{4(2)} 9$
$15 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3$，$15 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3$，$15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 8$
$15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 9$，$15 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13$，$15 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4$

因为 $N_1(S) \geq 2P_d + 1$，$N_2(S) \geq 2P_d + 1$，$N_3(S) \geq 2P_d + 1$，$N_4(S) \geq 2P_d + 1$ 和 $N_8(S) \geq 2P_d$，所以可能不满足 (2) 的 16 轮 GFC 肯定在下列的 36 种情形中。

$11 \xrightarrow{4(2)} 8 \xrightarrow{4(1)} 9 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3$
$15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 9 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3$
$14 \xrightarrow{4(2)} 11 \xrightarrow{4(2)} 9 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3$
$6 \xrightarrow{4(1)} 2 \xrightarrow{4(3)} 15 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3$
$6 \xrightarrow{4(1)} 2 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3$
$6 \xrightarrow{4(1)} 2 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 8$
$6 \xrightarrow{4(1)} 2 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 9$
$6 \xrightarrow{4(1)} 2 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13$
$6 \xrightarrow{4(1)} 2 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4$
$10 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3$
$10 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3$
$10 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 8$
$10 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 9$
$10 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13$
$10 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4$
$12 \xrightarrow{4(1)} 4 \xrightarrow{4(3)} 15 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3$
$12 \xrightarrow{4(1)} 4 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3$
$12 \xrightarrow{4(1)} 4 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 8$

$12 \xrightarrow{4(1)} 4 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 9$
$12 \xrightarrow{4(1)} 4 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13$
$12 \xrightarrow{4(1)} 4 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4$
$14 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3$
$14 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3$
$14 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 8$
$14 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 11 \xrightarrow{4(2)} 9$
$14 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13$
$14 \xrightarrow{4(2)} 6 \xrightarrow{4(3)} 15 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4$
$7 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3$
$7 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4$,
$7 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13$
$13 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3$
$13 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4$,
$13 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13$
$15 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13 \xrightarrow{4(2)} 5 \xrightarrow{4(2)} 3$
$15 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13 \xrightarrow{4(3)} 12 \xrightarrow{4(1)} 4$,
$15 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13 \xrightarrow{4(3)} 12 \xrightarrow{4(2)} 13$

首先需指出：从 16 轮 GFC 的结构知：$\Delta y_{12} = \Delta x_0 \oplus \Delta x_{16}$，$\Delta y_{16} = \Delta x_4 \oplus \Delta x_{20}$，$\Delta y_{20} = \Delta x_8 \oplus \Delta x_{24}$，$\Delta y_{24} = \Delta x_{12} \oplus \Delta x_{28}$，$\Delta y_{28} = \Delta x_{16} \oplus \Delta x_{32}$，$\Delta y_{32} = \Delta x_{20} \oplus \Delta x_{36}$，$\Delta y_{36} = \Delta x_{24} \oplus \Delta x_{40}$，$\Delta y_{40} = \Delta x_{28} \oplus \Delta x_{44}$，$\Delta y_{44} = \Delta x_{32} \oplus \Delta x_{48}$，$\Delta y_{48} = \Delta x_{36} \oplus \Delta x_{52}$，$\Delta y_{52} = \Delta x_{40} \oplus \Delta x_{54}$，$\Delta y_{56} = \Delta x_{44} \oplus \Delta x_{60}$，又从分支数 P_d 的定义可知：$H(\Delta y_i) + H(\Delta x_i) \geq P_d$。因此，我们有：$H_W(\Delta x_0) + H_W(\Delta x_{12}) + H_W(\Delta x_{16}) \geq P_d$，$H_W(\Delta x_4) + H_W(\Delta x_{16}) + H_W(\Delta x_{20}) \geq P_d$，$H_W(\Delta x_8) + H_W(\Delta x_{20}) + H_W(\Delta x_{24}) \geq P_d$，$H_W(\Delta x_{12}) + H_W(\Delta x_{24}) + H_W(\Delta x_{28}) \geq P_d$，$\cdots$，$H_W(\Delta x_{44}) + H_W(\Delta x_{56}) + H_W(\Delta x_{60}) \geq P_d$。

对 $11 \xrightarrow{4(2)} 8 \xrightarrow{4(1)} 9 \xrightarrow{4(3)} 7 \xrightarrow{4(2)} 3$ 由前面的讨论知：它的非 0 轮函数输入是 $\Delta x_0\Delta x_{12}\Delta x_{28}\Delta x_{32}\Delta x_{36}\Delta x_{40}\Delta x_{48}\Delta x_{52}$，因此它的活动盒子数为

$$\begin{aligned}&H_W(\Delta x_0)+H_W(\Delta x_{12})+H_W(\Delta x_{28})+H_W(\Delta x_{32})+H_W(\Delta x_{36})\\&\quad+H_W(\Delta x_{40})+H_W(\Delta x_{48})+H_W(\Delta x_{52})\\&=(H_W(\Delta x_0)+H_W(\Delta x_{12}))+(H_W(\Delta x_{32})+H_W(\Delta x_{36}))+(H_W(\Delta x_{40})\\&\quad+H_W(\Delta x_{52}))+H_W(\Delta x_{28})+H_W(\Delta x_{48})\geq P_d+P_d+P_d+2=3P_d+2\end{aligned}$$

证毕

对其它情形可以类似证明。

由引理 2 可得如下结果：

定理 1　(1) 如果轮函数是双射且它的最大差分和线性特征的概率分别是 p 和 q，则 16 轮 GFC 的差分和线性特征的概率上界为 p^7 和 q^7；

(2) 如果轮函数采用 SP 结构且是双射，S 盒的最大差分和线性特征的概率是 p_S 和 q_S，P 变换的分支数为 P_d，则 16 轮 GFC 的差分和线性特征的概率上界为 $(p_S)^{3P_d+1}$ 和 $(q_S)^{3P_d+1}$。

上面讨论了 16 轮的情况，对于 17 轮和 18 轮有如下结果：

推论 1　如果轮函数是双射且它的最大差分和线性特征的概率分别是 p 和 q，则 17 轮和 18 轮 GFC 的差分和线性特征的概率的上界为 p^8 和 q^8。

证明　详细分析 8 轮 GFC，我们列出不超过 6 个非零轮函数输入差分的所有可能：

$2 \xrightarrow{8(5)} 5$, $3 \xrightarrow{8(5)} 14(15)$, $4 \xrightarrow{8(5)} 12(13)$, $4 \xrightarrow{8(4)} 5$, $5 \xrightarrow{8(3)} 1$, $6 \xrightarrow{8(5)} 5$, $6 \xrightarrow{8(4)} 15$, $7 \xrightarrow{8(5)} 5(13)$, $7 \xrightarrow{8(4)} 4$, $7 \xrightarrow{8(3)} 1$, $8 \xrightarrow{8(4)} 7$, $8 \xrightarrow{8(5)} 14(15)$, $9 \xrightarrow{8(5)} 3$, $10 \xrightarrow{8(5)} 5(15)$, $10 \xrightarrow{8(3)} 2$, $11 \xrightarrow{8(3)} 9$, $11 \xrightarrow{8(5)} 3(7)$, $12 \xrightarrow{8(5)} 12(13)$, $12 \xrightarrow{8(4)} 15(5)$, $13 \xrightarrow{8(4)} 3(4)$, $13 \xrightarrow{8(5)} 5(13)$, $14 \xrightarrow{8(5)} 5(7,15)$, $14 \xrightarrow{8(4)} 8(9)$, $14 \xrightarrow{8(3)} 2$, $15 \xrightarrow{8(4)} 3(4)$, $15 \xrightarrow{8(5)} 3(5,6,8,9,13)$。

进一步，我们对 16 轮 GFC 列出不超过 9 个非零轮函数输入差分的所有可能：

$2 \xrightarrow{8(5)} 5 \xrightarrow{8(3)} 1$
$6 \xrightarrow{8(5)} 5 \xrightarrow{8(3)} 1$
$7 \xrightarrow{8(5)} 5 \xrightarrow{8(3)} 1$
$8 \xrightarrow{8(5)} 14 \xrightarrow{8(3)} 2$
$11 \xrightarrow{8(5)} 7 \xrightarrow{8(3)} 1$
$12 \xrightarrow{8(4)} 15 \xrightarrow{8(4)} 3(4)$
$14 \xrightarrow{8(3)} 2 \xrightarrow{8(5)} 5$
$14 \xrightarrow{8(4)} 8 \xrightarrow{8(4)} 7$

$3 \xrightarrow{8(5)} 14 \xrightarrow{8(3)} 2$
$6 \xrightarrow{8(4)} 15 \xrightarrow{8(4)} 3(4)$
$8 \xrightarrow{8(4)} 7 \xrightarrow{8(3)} 1$
$10 \xrightarrow{8(3)} 2 \xrightarrow{8(5)} 5$
$11 \xrightarrow{8(3)} 9 \xrightarrow{8(5)} 3$
$13 \xrightarrow{8(4)} 4 \xrightarrow{8(4)} 5$
$14 \xrightarrow{8(5)} 5 \xrightarrow{8(3)} 1$
$15 \xrightarrow{8(4)} 4 \xrightarrow{8(4)} 5$

$4 \xrightarrow{8(4)} 5 \xrightarrow{8(3)} 1$
$7 \xrightarrow{8(4)} 4 \xrightarrow{8(4)} 5$
$8 \xrightarrow{8(4)} 7 \xrightarrow{8(4)} 4$
$10 \xrightarrow{8(5)} 5 \xrightarrow{8(3)} 1$
$12 \xrightarrow{8(4)} 5 \xrightarrow{8(3)} 1$
$13 \xrightarrow{8(5)} 5 \xrightarrow{8(3)} 1$
$14 \xrightarrow{8(5)} 7 \xrightarrow{8(3)} 1$
$15 \xrightarrow{8(5)} 5 \xrightarrow{8(3)} 1$

又以 1 = (0 0 0 1) 为输入的 1, 2, 3 轮 GFC 的非零轮函数输入差分的个数的下界分别为 1, 2, 3；以 2 = (0 0 1 0) 为输入的 1, 2, 3 轮 GFC 的非零轮函数输入差分的个数的下界分别为 1, 2, 3；以 3 = (0 0 1 1) 为输入的 1, 2, 3 轮 GFC 的非零轮函数输入差分的个数的下界分别为 1, 1, 1；以 4 = (0 1 0 0) 为输入的 1, 2, 3 轮 GFC 的非零轮函数输入差分的个数的下界分别为 0, 0, 1。因此，17(18) 轮 GFC 的非零轮函数输入差分的个数的下界为 8。

证毕

3 结束语

由于差分和线性密码分析是目前最有效的攻击方法，因此，每个分组密码设计者都要想办法估计新算法抵抗差分和线性密码分析的能力．现有的做法是给出差分和线性特征的概率的上界．本文评估一类广义 Feistel 密码抵抗差分和线性密码分析的能力：如果轮函数是双射且它的最大差分和线性特征的概率分别是 p 和 q，则 16 轮 GFC 的差分和线性特征的概率的上界为 p^7 和 q^7；如果轮函数采用 SP 结构且是双射，S 盒的最大差分和线性特征的概率是 p_S 和 q_S，P 变换的分支数为 P_d，则 16 轮 GFC 的差分和线性特征的概率的上界为 $(p_S)^{3P_d+1}$ 和 $(q_S)^{3P_d+1}$．此工作的意义在于，以后设计采用 GFC 结构时，只需确定各个模块的密码特性就能估计整个算法抵抗差分和线性密码分析的能力．进一步要做的工作是讨论此类广义 Feistel 密码抵抗其它攻击的能力．另外，从本文的结果我们猜想：r(≥ 7) 轮 GFC 的非零轮函数输入差分的个数的下界为 $\lfloor \frac{r-2}{2} \rfloor$．希望有兴趣的同行证明之．

参 考 文 献

[1] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, Journal of Cryptology, 1991, 4(1), 3–72.

[2] M. Matsui, Linear cryptanalysis method for DES cipher, Advances in Cryptology-Eurocrypt'93 Proc., Berlin, Springer-Verlag, 1994, 386–397.

[3] J. Daemen, L. Kundsen, V. Rijmen, The Block Cipher Square, Fast Software Encryption, Berlin, Springer-Verlag, 1997, 149–165.

[4] L. R. Knudsen, Practically Secure Feistel Ciphers, Fast Software Encryption, New York, Springer-Verlag, 1994, 211–221.

[5] M. Kanda, Practical security evaluation against differential and linear attacks for Feistel ciphers with SPN round function, SAC'2000 Proc., Berlin, Springer-Verlag, 2000, 168–179.

[6] C. Adams, CAST-256, http://nist.gov/aes/.

SECURITY EVALUATION FOR A CLASS OF GENERALIZED FEISTEL CIPHERS

Wu Wenling He Yeping

(*State Key Lab of Info. Security, Institute of Software, CAS, Beijing* 100080, *China*)

(*Eng. Research Center for Info. Security Technology, CAS, Beijing* 100080, *China*)

Abstract This paper studies the security evaluation against differential and linear attacks for a class of generalized Feistel ciphers. If the round function is bijective and its maximum differential and linear characteristic probabilities are p and q, then the upper bounds of maximum differential and linear characteristic probabilities for 16-round ciphers are p^7 and q^7. If the round function is bijective and SP structure, the maximum differential and linear characteristic probabilities of S-boxes are p_S and q_S, the branch number of P is P_d, then the upper bounds of maximum differential and linear characteristic probabilities for 16-round ciphers are $(p_S)^{3P_d+1}$ and $(q_S)^{3P_d+1}$.

Key words Differential cryptanalysis, Linear cryptanalysis, Branch number, Cipher, S-box

吴文玲： 女，1966 年生，副研究员，研究方向为分组密码的设计与分析．

贺也平： 男，1962 年生，副研究员，研究方向为分组密码的设计与分析．