一类广义 Feistel 密码安全性能的进一步评估

王健康,王念平
(解放军信息工程大学密码工程学院,河南郑州 450004)

摘 要: 为评估一类广义 Feistel 密码的安全性能,利用迭代结构对该分组密码抵抗差分密码分析和线性密码分析的能力进行了深入的研究.在轮函数都是双射的假设条件下,证明了 4r(r≥1)轮广义 Feistel 密码至少有(8/3)r-[(rmod3)/3]+(rmod3)/3 个轮函数的输入差分非零.当 r ≥6 时,本文的结果比现有结果至少提高 20%.从而利用轮函数的最大差分和线性逼近概率,就可以估算出 4r(r≥1)轮广义 Feistel 密码最大差分特征概率和最大线性逼近概率的上界.

关键词: 广义 Feistel 密码; 差分特征; 线性特征; 概率
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2013) 10-1944-04
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.10.011

Further Security Evaluation for a Class of Generalized Feistel Ciphers

WANG Jian-kang, WANG Nian-ping
(*Institute of Crytography Engineering, the PLA Information Engineering University, Zhengzhou, Henan* 450004, *China*)

Abstract: To evaluate the security of a class of generalized Feistel ciphers, the security evaluation against differential and linear cryptanalyses is investigated deeply using iterative structure. If round functions are all bijective, then the number of active round functions for 4r-round (r≥1) ciphers are not less than (8/3)r-[(rmod3)/3]+(rmod3)/3. The result is at least improved 20% than the existing result when r≥6. So the upper bounds of maximum differential characteristic and linear approximation probabilities for 4r-round (r≥1) ciphers can be estimated if maximum differential and linear approximation probabilities for round function are given.

Key words: generalized Feistel ciphers; differential characteristic; linear characteristic; probabilities

1 引言

差分密码分析[1]和线性密码分析[2]是针对分组密码强有力的两种攻击方法.因此,每位分组密码设计者都要估计分组密码算法抵抗差分密码分析和线性密码分析的能力.常用的做法是给出最大差分特征概率和线性特征概率或给出差分特征概率和线性特征概率的上界.文献[3]给出了针对传统的 Feistel 密码的安全性评估.传统的 Feistel 密码大都是 64-bit 分组长度,而随着计算能力的提高,现在设计分组密码都要求至少是 128-bit 分组长度.而对于传统的 Feistel 密码,分组长度的增加意味着轮函数 F 规模的增加,而构造大规模的轮函数又是比较困难的,因此广义 Feistel 密码应运而生,例如图 1 所示的广义 Feistel 密码[4](简记为 GFC)就为我们设计分组密码创造了一条途径.文献[5-9]给出了一些广义 Feistel 密码的安全性评估.

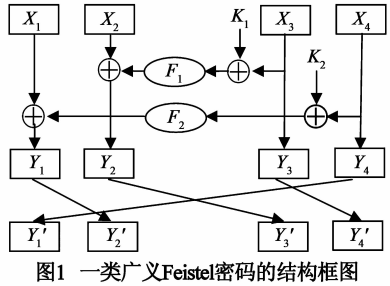

图1 一类广义Feistel密码的结构框图

文献[10]对图 1 所示的 GFC 的安全性能进行了初步的研究,证明了 4、8、12、16 轮 GFC 分别至少有 2、5、8、10 个轮函数的输入差分非零,并证明了 4r(r≥2)轮 GFC 至少有 2r+1 个轮函数的输入差分非零.从而若设轮函数的最大差分和线性特征的概率分别为 p 和 q,则 4r(r≥2)轮 GFC 的差分特征和线性特征的概率分别以 p^{2r+1} 和 q^{2r+1} 为其上界.本文经过进一步的分析,给出了 4r(r

收稿日期:2012-02-06;修回日期:2012-12-19;责任编辑:郭游
基金项目:国家自然科学基金(No.61202491,No.61272041,No.61272488)

≥1)轮 GFC 的差分特征和线性特征概率的一个新上界.

2 主要结论

在以下的分析中,假定轮函数 F_1 和 F_2 都是双射,并分别用 $X_i=(x_{4i+3},x_{4i+2},x_{4i+1},x_{4i})$ 和 $\Delta X_i=(\Delta x_{4i+3},\Delta x_{4i+2},\Delta x_{4i+1},\Delta x_{4i})(i\geqslant 0)$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,而用"0"表示零差分,"1"表示非零差分.因此,非零输入差分仅有 15 种表示,即 1=(0,0,0,1),…,15=(1,1,1,1).对于 4 轮 GFC,当输入差分为 1=(0,0,0,1)时,由 GFC 的结构可知:

$$1=(0,0,0,1)\rightarrow(1,1,0,0)\rightarrow(0,1,1,0)\rightarrow\begin{cases}(0,0,0,1)\rightarrow(1,1,0,0)=12\\(0,0,1,1)\rightarrow(1,1,1,1)=15\end{cases}$$

因为轮函数都是双射,所以输入差分非零时,输出差分一定非零,因此第 1 轮和第 2 轮比较清楚,即有 1=(0,0,0,1)→(1,1,0,0)→(0,1,1,0).对于第 3 轮,Δx_9 和 Δx_{10}都不为零,但 $F_1(\Delta x_9)$和 Δx_{10}有可能相等,也有可能不相等,从而第 3 轮的输出有两种情况:(0,0,0,1)或(0,0,1,1),相应地,第 4 轮输出也有两种情况:(1,1,0,0)或(1,1,1,1).为方便,我们用下列记号表示输入差分为 1=(0,0,0,1)的 4 轮 GFC:

$$1\begin{cases}\xrightarrow{4(3)}12\\\xrightarrow{4(4)}15\end{cases}$$

其中,箭头上方的数字 $u(v)$表示迭代 u 轮后,总共有 v 个轮函数的输入差分非零.类似地,可给出输入差分的每一个值经过 4 轮迭代后输出差分的所有取值情况:

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

$$4\xrightarrow{4(5)}9(11,13,15)\qquad 5\begin{cases}\xrightarrow{4(4)}5(7)\\\xrightarrow{4(5)}10(14)\\\xrightarrow{4(6)}9(11,13,15)\end{cases}$$

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

$$8\xrightarrow{4(3)}15\qquad 9\begin{cases}\xrightarrow{4(2)}3\\\xrightarrow{4(3)}12\\\xrightarrow{4(4)}15\end{cases}$$

$$10\begin{cases}\xrightarrow{4(5)}5(7)\\\xrightarrow{4(6)}8(10,12,14)\\\xrightarrow{4(7)}9(11,13,15)\end{cases}\qquad 11\begin{cases}\xrightarrow{4(5)}4(6)\\\xrightarrow{4(6)}5(7)\\\xrightarrow{4(7)}8(10,12,14)\\\xrightarrow{4(8)}9(11,13,15)\end{cases}$$

$$12\begin{cases}\xrightarrow{4(2)}6\\\xrightarrow{4(5)}9(11,13,15)\end{cases}\qquad 13\begin{cases}\xrightarrow{4(4)}5(7)\\\xrightarrow{4(5)}10(14)\\\xrightarrow{4(6)}9(11,13,15)\end{cases}$$

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

由上面的讨论可得以下引理:

引理 1　对于 4 轮 GFC,若轮函数都是双射,则

(1)至少有 2 个轮函数的输入差分非零;

(2)恰有 2 个轮函数的输入差分非零的情形只可能为:$9\xrightarrow{4(2)}3$、$12\xrightarrow{4(2)}6$;

(3)恰有 3 个轮函数的输入差分非零的情形只可能为:$1\xrightarrow{4(3)}12$、$6\xrightarrow{4(3)}1(3)$、$8\xrightarrow{4(3)}15$、$9\xrightarrow{4(3)}12$、$15\xrightarrow{4(3)}2$

引理 2　对于 8 轮 GFC,若轮函数都是双射,则

(1)至少有 5 个轮函数的输入差分非零;

(2)恰有 5 个轮函数的输入差分非零的情形只可能为:$12\xrightarrow{4(2)}6\xrightarrow{4(3)}1(3)$、$1\xrightarrow{4(3)}12\xrightarrow{4(2)}6$、$9\xrightarrow{4(3)}12\xrightarrow{4(2)}6$

证明　8 轮 GFC 可以拆分成前 4 轮和后 4 轮来讨论,由引理 1 易证该结论成立.　证毕

引理 3　对于 12 轮 GFC,当轮函数都是双射时,至少有 8 个轮函数的输入差分非零.

证明　12 轮 GFC 可以拆分成前 8 轮和后 4 轮来讨论,由引理 1 和引理 2 易证该结论成立.　证毕

定理 1　对于 $4r(r\geqslant 1)$轮 GFC,若轮函数都是双射,则至少有$(8/3)r-[(r\bmod 3)/3]+(r\bmod 3)/3$ 个轮函数的输入差分非零,其中 $r\bmod 3$ 表示 3 除 r 的非负余数,$[x]$表示不小于 x 的最小整数.

证明　(1)当 $r=3k(k\geqslant 1)$时.

此时,$4r=12k$,$(8/3)r-[(r\bmod 3)/3]+(r\bmod 3)/$

$3=8k$. 由引理 3 知,12 轮 GFC 至少有 8 个轮函数的输入差分非零,从而 $12k$ 轮 GFC 至少有 $8k$ 个轮函数的输入差分非零,本定理结论成立.

(2)当 $r=3k+1(k\geqslant 0)$时.

此时,$4r=12k+4$,$(8/3)r-[(r\bmod 3)/3]+(r\bmod 3)/3=8k+2$. 由引理 3 知,12 轮 GFC 至少有 8 个轮函数的输入差分非零,再由引理 1 知,4 轮 GFC 至少有两个轮函数的输入差分非零,从而 $12k+4$ 轮 GFC 至少有 $8k+2$ 个轮函数的输入差分非零,本定理结论成立.

(3)当 $r=3k+2(k\geqslant 0)$时.

此时,$4r=12k+8$,$(8/3)r-[(r\bmod 3)/3]+(r\bmod 3)/3=8k+5$. 由引理 3 知,12 轮 GFC 至少有 8 个轮函数的输入差分非零,再由引理 2 知,8 轮 GFC 至少有 5 个轮函数的输入差分非零,从而 $12k+8$ 轮 GFC 至少有 $8k+5$ 个轮函数的输入差分非零,本定理结论成立. 证毕

定理 2 如果轮函数都是双射且它的最大差分和线性逼近概率分别是 p 和 q,则 $4r(r\geqslant 1)$轮 GFC 的最大差分特征概率和线性特征的概率分别以 $p^{(8/3)r-[(r\bmod 3)/3]+(r\bmod 3)/3}$和 $q^{(8/3)r-[(r\bmod 3)/3]+(r\bmod 3)/3}$为其上界.

3 本文结果与文献[10]中结果的比较

文献[10]证明了 4、8、12、16 轮 GFC 分别至少有 2、5、8、10 个轮函数的输入差分非零,并证明了 $4r(r\geqslant 2)$ 轮 GFC 至少有 $2r+1$ 个轮函数的输入差分非零. 本文改进了文献[10]中的结果. 为直观起见,将本文的结果与文献[10]中的相应结果比较如下:

表 1 本文结果与文献[10]中结果的比较

轮数	4	8	12	16	20	24	28	32	36	…	$4r(r\geqslant 2)$
文献[10]中结果	2	5	8	10	11	13	15	17	19	…	$2r+1$
本文中的结果	2	5	8	10	13	16	18	21	24	…	$\frac{8}{3}r-\left[\frac{r\bmod 3}{3}\right]+\frac{r\bmod 3}{3}$
本文结果比文献[10]提高的百分比	0%	0%	0%	0%	18%	23%	20%	24%	26%	…	33%($r\to\infty$)

其中,33%($r\to\infty$)表示本文结果 $(8/3)r-[(r\bmod 3)/3]+(r\bmod 3)/3$ 比文献[10]中相应结果 $2r+1$ 提高的百分比的渐进值,即

$$\lim_{r\to\infty}\frac{((8/3)r-[(r\bmod 3)/3]+(r\bmod 3)/3)-(2r+1)}{2r+1}=\lim_{r\to\infty}\frac{(2/3)r-[(r\bmod 3)/3]-1+(r\bmod 3)/3}{2r+1}=\frac{1}{3}\approx 33\%$$

4 结束语

本文对一类广义 Feistel 密码抵抗差分密码分析和线性密码分析的能力进行了进一步地分析,给出了最大差分特征概率和线性特征概率的一个新上界,改进了文献[10]中的结果. 本文结果的意义在于:采用 GFC 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 和线性逼近概率 q 足够小,就能估计并保证整个算法抵抗差分密码分析和线性密码分析的能力. 进一步要做的工作是讨论该结构抵抗其它密码分析的能力.

参考文献

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

[2] M Matsui. Linear cryptanalysis method for DES cipher[A]. Proceedings of Advances in Cryptology-Eurocrypt′93[C]. Berlin: Springer-Verlag, 1993, 386 – 397.

[3] L R Knudsen. Practically secure Feistel Ciphers[A]. Proceedings of Fast Software Encryption[C]. Berlin: Springer-Verlag, 1994, 211 – 221.

[4] K Nyberg. Generalized Feistel networks[A]. Proceedings of Advances in Cryptology-ASIACRYPT′96[C]. Berlin: Springer-Verlag, 1996, 91 – 104.

[5] 余昭平,王念平. 一类非平衡 Feistel 网络的线性偏差分析[J]. 电子学报 2006, 34(7): 1231 – 1235.
Yu Zhao-ping, Wang Nian-ping. The linear deviation cryptanalysis for a kind of unbalanced feistel networks[J]. Acta Electronica Sinica, 2006, 34(7): 1231 – 1234. (in Chinese)

[6] 王念平,金晨辉,余昭平. 非平衡 Feistel 网络的线性可证明安全性的进一步分析[J]. 电子学报, 2006, 34(10): 1799 – 1803.
Wang Nian-ping, Jin Chen-hui, Yu zhao-ping. Furthermore Analyses of Linear Provable Security for a class of unbalanced Feistel Networks[J]. Acta Electronica Sinica, 2006, 34(10): 1799 – 1803. (in Chinese)

[7] 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.
Wu Wen-ling, He Ye-ping. Security evaluation for a class of Generalized Feistel Ciphers[J]. Journal of Electronics and Information Technology, 2002, 24(9): 1177 – 1184. (in Chinese)

[8] Y Kaneko, et al. On provable security against differential and linear cryptanalysis in generalized Feistel ciphers with multiple random functions[A]. Proceedings of SAC′97[C].

Berlin:Springer-Verlag,1997:185 – 199.

[9] 张如文.一类广义 Feistel 密码的线性分析[J].中国科学院研究生院学报,2003,20(1):31 – 38.
Zhang Ru-wen. Linear cryptanalysis for a class of Generalized Feistel Ciphers[J]. Journal of the Graduate School of the Chinese Academy of Science,2003,20(1):31 – 38.(in Chinese)

[10] 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 (4):63 – 67.
Wang Nian-ping. Security analysis for a class of Generalized Feistel Ciphers[J]. Journal of Dalian Maritime University,2007,33 (4):63 – 67.(in Chinese)

作者简介

王健康　男,1987 年出生于安徽淮北,现为信息工程大学密码工程学院硕士研究生,主要研究方向为密码学.
E-mail:jiankangwang@163.com

王念平　男,1973 年出生于河南洛阳,博士,硕士生导师,现为信息工程大学密码学副教授,主要研究方向为密码学.
E-mail:wwnnpp@126.com