四分组类 CLEFIA 变换簇抵抗差分密码分析的安全性评估

王念平
（解放军信息工程大学密码工程学院，河南郑州 450001）

摘 要： 差分密码分析是针对分组密码的强有力的攻击方法，估计分组密码抵抗差分密码分析的能力是分组密码安全性评估的重要内容之一. 基于实际应用背景，提出了“四分组类 CLEFIA 变换簇”的概念，并利用变换簇中两种特殊分组密码结构的差分对应之间的关系，给出了变换簇中所有密码结构抵抗差分密码分析的安全性评估结果.

关键词： 分组密码；四分组类 CLEFIA 变换簇；差分密码分析；活动轮函数
中图分类号： TN918.1 **文献标识码：** A **文章编号：** 0372-2112 (2017)10-2528-05
电子学报 URL： http://www.ejournal.org.cn **DOI：** 10.3969/j.issn.0372-2112.2017.10.030

Security Evaluation Against Differential Cryptanalysis for Four-Block CLEFIA-Like Transform Cluster

WANG Nian-ping
(*School of Cryptography Engineering, the PLA Information Engineering University, Zhengzhou, Henan* 450001, *China*)

Abstract: Differential cryptanalysis is a powerful attack on block ciphers and to evaluate the security against differential cryptanalysis is an important part for the security evaluation of block ciphers. Based on practical application background, the concept of four-block CLEFIA-like transform cluster is put forward. Using the relation between differential correspondences of two special block cipher structures, security evaluation against differential cryptanalysis for all block cipher structures of the cluster is given.

Key words: block ciphers; four-block CLEFIA-like transform cluster; differential cryptanalysis; active round function

1 引言

在分组密码的具体应用中，用户往往需要多样化的密码服务. 对于同类别但又不完全相同的应用，可以使用结构相似但又不尽相同的分组密码算法. “结构相似”，是为了实现方便；“结构不尽相同”，是为了提高安全性. 但如何保证这些“结构相似但又不尽相同”的分组密码算法的安全性，是分组密码算法设计者必须考虑的问题. 另一方面，差分密码分析[1,2]是针对分组密码的强有力的攻击方法，估计分组密码抵抗差分密码分析的能力，是分组密码设计者不可回避的问题. 基于此，本文提出了“四分组类 CLEFIA 变换簇”的概念，并通过对变换簇的研究，给出了变换簇中所有分组密码结构（而不仅仅是一种分组密码结构）抵抗差分密码分析的安全性评估结果. 这种“四分组类 CLEFIA 变换簇”基于常用的广义 Feistel 结构[3-5]，其中的块移位变换设计成循环左移变换或循环右移变换，且不同轮中的块移位变换可以相同也可以不同. 显然，块移位变换设计得不同，得到的广义 Feistel 结构也不同，这些不同的广义 Feistel 结构共同构成一簇变换，称为“四分组类 CLEFIA 变换簇”.

本文的结构安排是这样的：第 1 节是引言部分；第 2 节给出有关的定义和引理；第 3 节给出基于循环左移和循环右移变换的“四分组类 CLEFIA 变换簇”的描述；第 4 节给出四分组类 CLEFIA 变换簇抵抗差分密码分析的安全性评估结果；第 5 节是结束语.

2 有关的定义和引理

Y. Zheng 等人[6]提出了 Type-II 型广义 Feistel 结

收稿日期：2016-01-22；修回日期：2017-05-26；责任编辑：郭游
基金项目：国家自然科学基金（No. 61672031, No. 61402523, No. 61572516）

构,T. Shirai 等人[7]利用该结构设计了 CLEFIA 算法. 本文提出图 1 所示的四分组类 CLEFIA 结构. 其中,块移位变换 P 可以是循环左移变换(1,2,3,4)→(2,3,4,1),也可以是循环右移变换(1,2,3,4)→(4,1,2,3),且不同轮中的块移位变换可以不同.

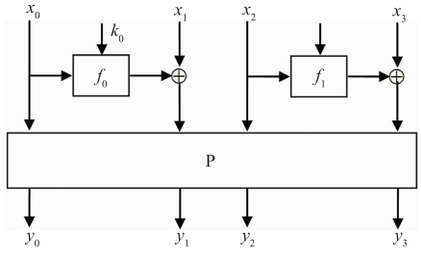

图1　四分组类CLEFIA结构

定义 1[6]　设 $x_i, k_j \in Z_2^n, 0 \leqslant i \leqslant 3, 0 \leqslant j \leqslant 1$,圈函数为

$$Q_k(x_0, x_1, x_2, x_3) =$$
$$P(x_0, x_1 \oplus f_0(x_0 \oplus k_0), x_2, x_3 \oplus f_1(x_2 \oplus k_1))$$

的结构称为四分组类 CLEFIA 结构. 其中 $Z_2^n = \{(z_0, z_1, \cdots, z_{n-1}) \mid z_i = 0,1, 0 \leqslant i \leqslant n-1\}$,$P$ 是关于分块 $x_0, x_1 \oplus f_0(x_0 \oplus k_0), x_2, x_3 \oplus f_1(x_2 \oplus k_1)$ 的循环左移变换或循环右移变换,"⊕"表示异或运算,$k = (k_0, k_1)$ 表示轮密钥,$f_j: Z_2^n \to Z_2^n (0 \leqslant j \leqslant 1)$ 统称为 f 函数或轮函数.

定义 2[8]　设 $(X, +)$ 和 $(Y, +)$ 都是有限交换群,$f: X \to Y, \alpha \in X, \beta \in Y$,令

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

则称 $p_f(\alpha \to \beta)$ 为 f 在输入差为 α 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. 这里,"+"表示群 $(X, +)$ 中的群运算,$|X|$ 和 $\#\{\cdot\}$ 都表示集合的元素个数.

显然,差分对应 0→0 的概率恒为 1,此时,称 0→0 为平凡差分对应,否则称为非平凡差分对应. 以下考虑的都是非平凡的情形.

定义 3[9]　设 $\alpha \to \beta$ 是四分组类 CLEFIA 结构的 f 函数的一个差分对应,若 $\alpha \neq 0$,则称 f 函数是活动的.

引理 1[10]　对图 1 所示的四分组类 CLEFIA 结构,设轮函数都是双射,且块移位变换都是循环左(右)移变换,则 $r(r \geqslant 1)$ 轮差分特征至少有 $r - [(r \bmod 6)/6]$ 个活动轮函数. 其中,$r \bmod 6$ 表示 r 除以 6 的最小非负余数,$[x]$ 表示不小于 x 的最小整数.

3　四分组类 CLEFIA 变换簇

为叙述方便起见,用 $(i_1 i_2 i_3 i_4)$ 表示 4 元置换 $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix}$,即元素 j 经过置换后的像 $\varphi(j) = i_j (j = 1,2,3,4)$. 按照这种表示方法,循环左移变换和循环右移变换可分别表示为(2341)和(4123).

下面给出四分组类 CLEFIA 变换簇的描述.

用 C^n 表示 $4n(n \geqslant 1)$ 轮四分组类 CLEFIA 结构. 按照从第 1 轮到第 $4n$ 轮的顺序,依次将每 4 轮看成一个"单元",用 G_1 表示第 1 轮到第 4 轮,G_2 表示第 5 轮到第 8 轮,…,G_n 表示第 $4n-3$ 轮到第 $4n$ 轮,从而 C^n 可表示成 $C^n = G_n \cdot G_{n-1} \cdot \cdots \cdot G_2 \cdot G_1$. 这里,"·"表示变换的复合. 在同一个"单元" $G_i (1 \leqslant i \leqslant n)$ 内,每一轮中的块移位变换都是相同的(不妨记这一相同的变换为 $P_i (1 \leqslant i \leqslant n)$),要么都为循环左移变换 $p_1 = (2341)$,要么都为循环右移变换 $p_2 = (4123)$. 而对不同的"单元",使用的块移位变换可以相同,也可以不同,但也只能从循环左移变换 $p_1 = (2341)$ 和循环右移变换 $p_2 = (4123)$ 中选取. 也就是说,同一"单元"中的块移位变换都相同,不同"单元"中的块移位变换可以相同也可以不同,但其中的块移位变换只能为循环左移变换或循环右移变换.

因任一"单元" $G_i (1 \leqslant i \leqslant n)$ 中的块移位变换有两种选择,即循环左移变换和循环右移变换,故 $4n(n \geqslant 1)$ 轮四分组类 CLEFIA 结构共有 2^n 种,这 2^n 种结构共同构成一个变换簇,称为四分组类 CLEFIA 变换簇,记作 $M^n = \{C^n \mid C^n = G_n \cdot G_{n-1} \cdot \cdots \cdot G_2 \cdot G_1, P_i \in \{p_1, p_2\}, 1 \leqslant i \leqslant n\}$. 其中,$M^n$ 中的每一个元素 C^n 都表示一个 $4n$ 轮四分组类 CLEFIA 结构.

4　四分组类 CLEFIA 变换簇抵抗差分密码分析的安全性评估

为叙述方便起见,记块移位变换都为循环左移变换(2341)的四分组类 CLEFIA 结构为 CLEFIA-(2341),记块移位变换都为循环右移变换(4123)的四分组类 CLEFIA 结构为 CLEFIA-(4123). 显然,四分组类 CLEFIA 结构 CLEFIA-(2341)的圈函数为 $Q_k(x_0, x_1, x_2, x_3) = (x_1 \oplus f_0(x_0 \oplus k_0), x_2, x_3 \oplus f_1(x_2 \oplus k_1), x_0)$,四分组类 CLEFIA 结构 CLEFIA-(4123)的圈函数为 $Q_k(x_0, x_1, x_2, x_3) = (x_3 \oplus f_1(x_2 \oplus k_1), x_0, x_1 \oplus f_0(x_0 \oplus k_0), x_2)$.

本节具体安排如下:首先,给出四分组类 CLEFIA 结构 CLEFIA-(2341)和 CLEFIA-(4123)的差分对应的结构形式;其次,利用所得到的差分对应的结构形式,给出关于 CLEFIA-(2341)和 CLEFIA-(4123)的 2 轮差分特征的两个引理;最后,利用这两个引理,给出四分组类 CLEFIA 变换簇抵抗差分密码分析的安全性评估结果.

首先,易知四分组类 CLEFIA 结构 CLEFIA-(2341)的具有非零概率的差分对应都具有形式 $(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$

$\rightarrow(\alpha_1\oplus\beta_0,\alpha_2,\alpha_3\oplus\beta_1,\alpha_0)$,且轮函数$f_0$和$f_1$相应的差分对应分别为$\alpha_0\rightarrow\beta_0$和$\alpha_2\rightarrow\beta_1$;四分组类CLEFIA结构CLEFIA-(4123)的具有非零概率的差分对应都具有形式$(\alpha_0,\alpha_1,\alpha_2,\alpha_3)\rightarrow(\alpha_3\oplus\beta_1,\alpha_0,\alpha_1\oplus\beta_0,\alpha_2)$,且轮函数$f_0$和$f_1$相应的差分对应分别为$\alpha_0\rightarrow\beta_0$和$\alpha_2\rightarrow\beta_1$.

其次,给出关于CLEFIA-(2341)和CLEFIA-(4123)的2轮差分特征的两个引理.

在以下的分析中,假设两种四分组类CLEFIA结构CLEFIA-(2341)和CLEFIA-(4123)的轮函数f_0和f_1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. 注意,这里并不考虑具体的差分值,而用"0"表示零差分,用"1"表示非零差分. 因此,非零差分有且仅有15种表示,即1=(0,0,0,1),2=(0,0,1,0),…,15=(1,1,1,1).

例如,对于四分组类CLEFIA结构CLEFIA-(2341),当输入差分为10=(1,0,1,0)时,长度为2的差分特征可用上述方法描述如下:

$$10=(1,0,1,0)\rightarrow(1,1,1,1)\rightarrow\begin{cases}(0,1,0,1)=5\\(0,1,1,1)=7\\(1,1,0,1)=13\\(1,1,1,1)=15\end{cases}$$

事实上,因为四分组类CLEFIA结构CLEFIA-(2341)的轮函数都是双射,所以输入差分非零时,输出差分一定非零,因此第1轮比较清楚,即有10=(1,0,1,0)→(1,1,1,1). 对于第2轮,Δx_5和Δx_7都不为零,但$f_0(\Delta x_7)$(即$f_0(x_7)\oplus f_1(x'_7)$)和Δx_6有可能相等,也有可能不相等,$f_1(\Delta x_5)$(即$f_1(x_5)\oplus f_1(x'_5)$)和Δx_4有可能相等,也有可能不相等,从而第2轮的输出有4种情况:(0,1,0,1),(0,1,1,1),(1,1,0,1)或(1,1,1,1).

为了方便起见,用下列记号表示上述的输入差分10=(1,0,1,0)经过两轮迭代后输出差分的取值情况:$10\xrightarrow{1(2)}15\xrightarrow{1(2)}5(7,13,15)$. 其中,$\alpha\xrightarrow{u(v)}\beta$表示输入差分$\alpha$经过$u(u\geqslant 1)$轮迭代后,总共有$v(v\geqslant 0)$个轮函数的输入差分非零(即有$v$个轮函数是活动的). 类似地,可以给出非零输入差分的每一个值经过2轮*CLEFIA*-(2341)迭代后输出差分的所有取值情况:

$1\xrightarrow{1(0)}2\xrightarrow{1(1)}6$ $2\xrightarrow{1(1)}6\xrightarrow{1(1)}14$ $3\begin{cases}\xrightarrow{1(1)}4\xrightarrow{1(0)}8\\\xrightarrow{1(1)}6\xrightarrow{1(1)}14\end{cases}$

$4\xrightarrow{1(0)}8\xrightarrow{1(1)}9$ $5\xrightarrow{1(0)}10\xrightarrow{1(2)}15$ $6\xrightarrow{1(1)}14\xrightarrow{1(2)}7(15)$

$7\begin{cases}\xrightarrow{1(1)}12\xrightarrow{1(1)}1(9)\\\xrightarrow{1(1)}14\xrightarrow{1(2)}7(15)\end{cases}$ $8\xrightarrow{1(1)}9\xrightarrow{1(1)}11$

$9\xrightarrow{1(1)}11\xrightarrow{1(2)}13(15)$ $10\xrightarrow{1(2)}15\xrightarrow{1(2)}5(7,13,15)$

$11\begin{cases}\xrightarrow{1(2)}13\xrightarrow{1(1)}3(11)\\\xrightarrow{1(2)}15\xrightarrow{1(2)}5(7,13,15)\end{cases}$ $12\begin{cases}\xrightarrow{1(1)}1\xrightarrow{1(0)}2\\\xrightarrow{1(1)}9\xrightarrow{1(1)}11\end{cases}$

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

$15\begin{cases}\xrightarrow{1(2)}5\xrightarrow{1(0)}10\\\xrightarrow{1(2)}7\xrightarrow{1(1)}12(14)\\\xrightarrow{1(2)}13\xrightarrow{1(1)}3(11)\\\xrightarrow{1(2)}15\xrightarrow{1(2)}5(7,13,15)\end{cases}$

同样地,可以给出非零输入差分的每一个值经过2轮CLEFIA-(4123)迭代后输出差分的所有取值情况:

$1\xrightarrow{1(0)}8\xrightarrow{1(1)}6$ $2\xrightarrow{1(1)}9\xrightarrow{1(1)}14$ $3\begin{cases}\xrightarrow{1(1)}1\xrightarrow{1(0)}8\\\xrightarrow{1(1)}9\xrightarrow{1(1)}14\end{cases}$

$4\xrightarrow{1(0)}2\xrightarrow{1(1)}9$ $5\xrightarrow{1(0)}10\xrightarrow{1(2)}15$ $6\xrightarrow{1(1)}11\xrightarrow{1(2)}7(15)$

$7\begin{cases}\xrightarrow{1(1)}3\xrightarrow{1(1)}1(9)\\\xrightarrow{1(1)}11\xrightarrow{1(2)}7(15)\end{cases}$ $8\xrightarrow{1(1)}6\xrightarrow{1(1)}11$

$9\xrightarrow{1(1)}14\xrightarrow{1(2)}13(15)$ $10\xrightarrow{1(2)}15\xrightarrow{1(2)}5(7,13,15)$

$11\begin{cases}\xrightarrow{1(2)}7\xrightarrow{1(1)}3(11)\\\xrightarrow{1(2)}15\xrightarrow{1(2)}5(7,13,15)\end{cases}$ $12\begin{cases}\xrightarrow{1(1)}4\xrightarrow{1(0)}2\\\xrightarrow{1(1)}6\xrightarrow{1(1)}11\end{cases}$

$13\begin{cases}\xrightarrow{1(1)}12\xrightarrow{1(1)}4(6)\\\xrightarrow{1(1)}14\xrightarrow{1(2)}13(15)\end{cases}$ $14\begin{cases}\xrightarrow{1(2)}13\xrightarrow{1(1)}12(14)\\\xrightarrow{1(2)}15\xrightarrow{1(2)}5(7,13,15)\end{cases}$

$15\begin{cases}\xrightarrow{1(2)}5\xrightarrow{1(0)}10\\\xrightarrow{1(2)}13\xrightarrow{1(1)}12(14)\\\xrightarrow{1(2)}7\xrightarrow{1(1)}3(11)\\\xrightarrow{1(2)}15\xrightarrow{1(2)}5(7,13,15)\end{cases}$

由上面的讨论容易验证以下引理2成立.

引理2 对于四分组类CLEFIA结构CLEFIA-(2341)和CLEFIA-(4123),设轮函数都是双射,则

(1)设$\alpha\xrightarrow{1(u)}\delta(\alpha\neq 0)$是CLEFIA-(2341)的1轮差分特征,$\alpha\xrightarrow{1(s)}\xi(\alpha\neq 0)$是CLEFIA-(4123)的1轮差分特征,则$u=s$.

(2)对于相同的非零输入差分α,CLEFIA-(2341)经过2轮迭代后的输出差分和CLEFIA-(4123)经过2轮迭代后的输出差分相同;

(3)设$\alpha\xrightarrow{1(u)}\delta\xrightarrow{1(v)}\beta(\alpha\neq 0)$是CLEFIA-(2341)的2轮差分特征,$\theta\xrightarrow{1(s)}\xi\xrightarrow{1(t)}\eta(\theta\neq 0)$是CLEFIA-

(4123)的 2 轮差分特征. 若 $\alpha=\theta,\beta=\eta$,则 $u=s,v=t$,进而 $u+v=s+t$.

引理 2(1)实际上是说:若 CLEFIA-(2341)和 CLEFIA-(4123)的 1 轮差分特征的非零输入差分相同,则活动轮函数的个数也相同,即 $u=s$.

引理 2(3)实际上是说:若 CLEFIA-(2341)和 CLEFIA-(4123)的 2 轮差分特征的非零输入差分相同,输出差分也相同,则 CLEFIA-(2341)和 CLEFIA-(4123)经过每 1 轮迭代后相应的活动轮函数的个数都相同,即 $u=s,v=t$. 此时,CLEFIA-(2341)的 2 轮差分特征 $\alpha\xrightarrow{1(u)}\delta\xrightarrow{1(v)}\beta(\alpha\neq0)$ 和 CLEFIA-(4123)的 2 轮差分特征 $\theta\xrightarrow{1(s)}\xi\xrightarrow{1(t)}\eta(\theta\neq0)$ 中活动轮函数的个数也相同,即 $u+v=s+t$.

引理 3　对于四分组类 CLEFIA 结构 CLEFIA-(2341)和 CLEFIA-(4123),设轮函数都是双射,则 CLEFIA-(2341)存在差分特征 $\alpha\xrightarrow{2(u)}\beta(\alpha\neq0)$ 当且仅当 CLEFIA-(4123)存在差分特征 $\alpha\xrightarrow{2(u)}\beta(\alpha\neq0)$.

证明　设 CLEFIA-(2341)存在差分特征 $\alpha\xrightarrow{2(u)}\beta$. 由引理 2(2)知,CLEFIA-(4123)也存在差分特征 $\alpha\xrightarrow{2(s)}\beta$,再由引理 2(3)知 $u=s$,即 CLEFIA-(4123)也存在差分特征 $\alpha\xrightarrow{2(u)}\beta$,反之亦然,故本引理结论成立. 证毕

最后,利用引理 2、引理 3 以及引理 1,给出四分组类 CLEFIA 变换簇抵抗差分密码分析的安全性评估结果.

定理 1　设 M^n 是四分组类 CLEFIA 变换簇,C^n 是 M^n 中任一 $4n$ 轮四分组类 CLEFIA 结构,且设轮函数都是双射,则 C^n 的 $r(1\leqslant r\leqslant 4n)$ 轮差分特征至少有 $r-[(r\bmod 6)/6]$ 个活动轮函数. 其中,M^n 和 C^n 的具体含义见第 3 节,$r\bmod 6$ 表示 r 除以 6 的最小非负余数,$[x]$ 表示不小于 x 的最小整数.

证明　显然,$r=1$ 时,$r-[(r\bmod 6)/6]=0$,定理结论自然成立,故以下假设 $r\geqslant 2$.

由引理 1 知,要想证明本定理结论成立,只需证明 C^n 的 r 轮差分特征与 CLEFIA-(2341)的 r 轮差分特征具有相同的活动轮函数个数的下界,而要证明这一点,只需证明:CLEFIA-(2341)存在一条 r 轮差分特征当且仅当 C^n 也存在一条具有同样多个活动轮函数的 r 轮差分特征.

下面根据差分特征的轮数 r 的奇偶性分两种情形进行证明.

情形之一:$r=2k(1\leqslant k\leqslant 2n)$ 时.

此时,由引理 3 知,CLEFIA-(2341)存在 2 轮差分特征 $\alpha\xrightarrow{2(u)}\beta$ 当且仅当 CLEFIA-(4123)也存在差分特征 $\alpha\xrightarrow{2(u)}\beta$,从而,由 C^n 的含义知,CLEFIA-(2341)存在 r 轮差分特征 $\alpha_1\xrightarrow{2(u_1)}\alpha_2\xrightarrow{2(u_2)}\alpha_3\xrightarrow{2(u_3)}\cdots\xrightarrow{2(u_{k-1})}\alpha_k\xrightarrow{2(u_k)}\alpha_{k+1}$ 当且仅当 C^n 也存在 r 轮差分特征 $\alpha_1\xrightarrow{2(u_1)}\alpha_2\xrightarrow{2(u_2)}\alpha_3\xrightarrow{2(u_3)}\cdots\xrightarrow{2(u_{k-1})}\alpha_k\xrightarrow{2(u_k)}\alpha_{k+1}$,其中 $k=\frac{r}{2}$. 从而,C^n 的 r 轮差分特征与 CLEFIA-(2341)的 r 轮差分特征具有相同的活动轮函数个数的下界.

情形之二:$r=2k+1(1\leqslant k\leqslant 2n-1)$ 时.

此时,由 $r=2k+1$ 知 $r-1=2k$,故 $r-1$ 是偶数,从而由情形之一的证明过程知,CLEFIA-(2341)存在 $r-1$ 轮差分特征 $\alpha_1\xrightarrow{2(u_1)}\alpha_2\xrightarrow{2(u_2)}\alpha_3\xrightarrow{2(u_3)}\cdots\xrightarrow{2(u_{k-1})}\alpha_k\xrightarrow{2(u_k)}\alpha_{k+1}$ 当且仅当 C^n 也存在 $r-1$ 轮差分特征 $\alpha_1\xrightarrow{2(u_1)}\alpha_2\xrightarrow{2(u_2)}\alpha_3\xrightarrow{2(u_3)}\cdots\xrightarrow{2(u_{k-1})}\alpha_k\xrightarrow{2(u_k)}\alpha_{k+1}$,其中 $k=\frac{(r-1)}{2}$.

再设 $\alpha_{k+1}\xrightarrow{1(v)}\alpha_{k+2}(v\geqslant 0)$ 是 CLEFIA-(2341)的 1 轮差分特征,$\alpha_{k+1}\xrightarrow{1(s)}\xi(s\geqslant 0)$ 是 CLEFIA-(4123)的 1 轮差分特征(注:由引理 2(1)知 $v=s$),则由 C^n 的含义知,CLEFIA-(2341)存在 r 轮差分特征 $\alpha_1\xrightarrow{2(u_1)}\alpha_2\xrightarrow{2(u_2)}\alpha_3\xrightarrow{2(u_3)}\cdots\xrightarrow{2(u_{k-1})}\alpha_k\xrightarrow{2(u_k)}\alpha_{k+1}\xrightarrow{1(v)}\alpha_{k+2}$ 当且仅当以下两个条件之一成立:

(A)C^n 存在 r 轮差分特征 $\alpha_1\xrightarrow{2(u_1)}\alpha_2\xrightarrow{2(u_2)}\alpha_3\xrightarrow{2(u_3)}\cdots\xrightarrow{2(u_{k-1})}\alpha_k\xrightarrow{2(u_k)}\alpha_{k+1}\xrightarrow{1(v)}\alpha_{k+2}$;

(B)C^n 存在 r 轮差分特征 $\alpha_1\xrightarrow{2(u_1)}\alpha_2\xrightarrow{2(u_2)}\alpha_3\xrightarrow{2(u_3)}\cdots\xrightarrow{2(u_{k-1})}\alpha_k\xrightarrow{2(u_k)}\alpha_{k+1}\xrightarrow{1(s)}\xi$.

当条件(A)成立时,自然恒有 $u_1+u_2+u_3+\cdots+u_{k-1}+u_k+v=u_1+u_2+u_3+\cdots+u_{k-1}+u_k+v$;当条件(B)成立时,由引理 4.1(1)知 $v=s$,故必有 $u_1+u_2+u_3+\cdots+u_{k-1}+u_k+v=u_1+u_2+u_3+\cdots+u_{k-1}+u_k+s$. 这样就证明了:CLEFIA-(2341)存在一条 r 轮差分特征当且仅当 C^n 也存在一条具有同样多个活动轮函数的 r 轮差分特征,从而 C^n 的 r 轮差分特征与 CLEFIA-(2341)的 r 轮差分特征具有相同的活动轮函数个数的下界.

由情形之一和情形之二知,C^n 的 r 轮差分特征与 CLEFIA-(2341)的 r 轮差分特征具有相同的活动轮函数

个数的下界,再由引理 1 即知本定理结论成立. 证毕

定理 1 的重要意义在于:给出了四分组类 CLEFIA 变换簇中所有 2^n 种(而不仅仅是一种)分组密码结构抵抗差分密码分析的安全性评估结果. 不难看出,定理 1 的证明主要是利用了四分组类 CLEFIA 结构 CLEFIA-(2341)和 CLEFIA-(4123)的差分对应之间的关系.

定理 2 设 M^n 是四分组类 CLEFIA 变换簇,C^n 是 M^n 中任一 $4n$ 轮四分组类 CLEFIA 结构,再设轮函数都是双射且轮函数的最大差分概率为 $p_{\max}$,则 C^n 的 $r(1\leqslant r\leqslant 4n)$ 轮差分特征概率 $\leqslant [p_{\max}]^{r-[(r \bmod 6)/6]}$.

5 结束语

本文提出了四分组类 CLEFIA 变换簇,并利用变换簇中两种特殊分组密码结构的差分对应之间的关系,给出了变换簇中所有密码结构(而不仅仅是一种)抵抗差分密码分析的安全性评估结果. 本文的结果,希望对分组密码算法的设计和分析具有一定的指导意义.

参考文献

[1] Eli Biham, Adi Shamir. Differential cryptanalysis of DES-like cryptosystems[A]. Proceedings of Advances in Cryptology-CRYPT0'90[C]. LNCS 537, Berlin: Springer-Verlag, 1991. 3 – 72.

[2] Xuejia Lai, James L Massey, Sean Murphy. Markov ciphers and differential cryptanalysis[A]. Proceedings of Advances in Cryptology – EUROCRYPT'91[C]. LNCS 547, Berlin: Springer-verlag, 1991. 17 – 38.

[3] Kyoji Shibutani. On the diffusion of generalized Feistel structures regarding differential and linear cryptanalysis [A]. Proceedings of Selected Areas in Cryptography-SAC'10[C]. LNCS 6544, Berlin: Springer-Verlag, 2011: 211 – 228.

[4] 王健康,王念平. 一类广义 Feistel 密码安全性能的进一步评估[J]. 电子学报,2013,41(10):1944 – 1947.
Wang Jian-kang, Wang Nian-ping. Further security evaluation for a class of generalized Feistel ciphers[J]. Acta Electronica Sinica, 2013, 41(10): 1944 – 1947. (in Chinese).

[5] 王念平,殷勍. SMS4 型密码结构抵抗差分和线性密码分析能力评估[J]. 密码学报,2015,2(2):189 – 196.
Wang N P, Yin Q. Security evaluation for SMS4-typed ciphers structure against differential and linear cryptanalysis [J]. Journal of Cryptologic Research, 2015, 2(2): 189 – 196. (in Chinese)

[6] Yuliang Zheng, Tsutomu Matsumoto, Hideki Imai. On the construction of block ciphers provable secure and not relying on any unproven hypotheses[A]. Proceedings of Advances in Cryptology-CRYPTO'89[C]. LNCS 435, New York: Springer-verlag, 1990. 461 – 480.

[7] Taizo Shirai, Kyoji Shibutani, Toru Akishita, et al. The 128-Bit blockcipher CLEFIA[A]. Proceedings of Fast Software Encryption-FSE'07[C]. LNCS 4593, Berlin: Springer-Verlag, 2007: 181 – 195.

[8] 金晨辉,郑浩然,张少武等. 密码学[M]. 北京:高等教育出版社,2009.
Jin Chen-hui, Zheng Hao-ran, Zhang Shao-wu et al . Cryptology[M]. Beijing: Higher Education Press, 2009. (in Chinese)

[9] Bruce Schneier, John Kelsey. Unbalanced Feistel networks and block cipher design[A]. In: Proceedings of Fast Software Encryption-FSE'96[C]. LNCS 1039, Berlin: Springer-Verlag, 1996. 121 – 144.

[10] 王健康,王念平. 一类分组密码的安全性能评估[J]. 密码与信息安全学报,2012,24(5):7 – 11.
Wang Jian-kang, Wang Nian-ping. Security evaluation for a class of block ciphers[J]. Journal of Cryptology and Information Security, 2012, 24(5): 7 – 11. (in Chinese)

作者简介

王念平 男,1973 年生于河南洛阳,博士,教授,博士生导师,主要研究领域为密码学和信息安全.

E-mail :wwnnpp@126.com