一类分组密码变换簇抵抗线性密码分析的安全性评估

王念平
（中国人民解放军战略支援部队信息工程大学，河南郑州 450001）

摘 要： 线性密码分析是针对分组密码的强有力的攻击方法，估计分组密码抵抗线性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线性逼近之间的关系，给出了变换簇中所有密码结构抵抗线性密码分析的安全性评估结果，并提出了需要进一步探讨的若干问题. 这种利用变换簇对分组密码进行研究的方法，为分组密码的安全性评估提供了一个较为新颖的思路.

关键词： 分组密码；四分组类 CLEFIA 变换簇；线性密码分析；活动轮函数
中图分类号： TN918.1 **文献标识码：** A **文章编号：** 0372-2112 (2020)01-0137-06
电子学报 URL： http://www.ejournal.org.cn **DOI：** 10.3969/j.issn.0372-2112.2020.01.017

Security Evaluation Against Linear Cryptanalysis for a Class of Block Cipher Transform Cluster

WANG Nian-ping
(*The PLA Strategic Support Force Information Engineering University, Zhengzhou, Henan* 450001, *China*)

Abstract: Linear cryptanalysis is a powerful attack on block ciphers. To evaluate the security against linear cryptanalysis is one of the most important part for the security evaluation of block ciphers. In this paper, the concept of four-block CLEFIA-like transform cluster is put forward based on the background of practical application. Using the relation between linear approximations of two special block cipher structures, security evaluation against linear cryptanalysis for all block cipher structures of the cluster is given. Moreover, some open problems are given. We provide a novel idea for the security evaluation of block ciphers by using transform cluster to study block ciphers.

Key words: block ciphers; four-block CLEFIA-like transform cluster; linear 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，线性密码分析[1]是针对分组密码的强有力的攻击方法，估计分组密码抵抗线性密码分析的能力，是分组密码设计者必须考虑的问题. 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）抵抗线性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[2]，其中的块移位变换设计成循环左移变换或循环右移变换，且某些轮中的块移位变换可以不同. 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”. 顺便指出，本文之所以选取四分组类 CLEFIA 结构作为研究对象，主要是该结构属于典型的广义 Feistel 结构，有着良好的应用背景，例如 CLEFIA[3]算法就是采用该结构设计的. 当

收稿日期：2018-03-19；修回日期：2019-06-17；责任编辑：郭游
基金项目：国家自然科学基金（No. 61672031, No. 61402523, No. 61572516）

然,对于其它的广义 Feistel 结构(如 SMS4 结构[4]),也可以类似地构成密码变换簇,但这些密码变换簇抵抗线性密码分析的能力如何,需要进一步的分析.

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 变换簇抵抗线性密码分析的安全性评估结果;第 5 节提出需要进一步探讨的若干问题;第 6 节是结束语.

2 有关的定义和引理

Zheng Y 等人[5]提出了 Type-II 型广义 Feistel 结构,Shirai T 等人[3]利用该结构设计了 CLEFIA 算法. 为叙述方便起见,本文称 Type-II 型广义 Feistel 结构为 CLEFIA 结构,图 1 所示的是输入分成四个分块的情形,即四分组 CLEFIA 结构. 其中,轮函数 f_0 和 f_1 可采用 SP 结构(Substitution-Permutation Structures,替换-置换结构)或 SPS 结构(Substitution-Permutation-Substitution Structures,替换-置换-替换结构).

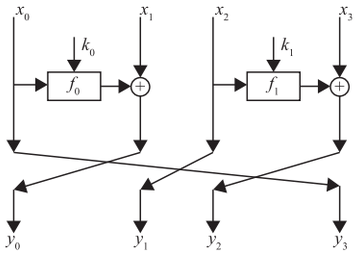

图1 四分组CLEFIA结构

图 1 中的块移位变换采用循环左移变换,当然,循环左移变换也可以用其它的块移位变换代替,形成图 2 所示的四分组类 CLEFIA 结构. 其中,不同轮中的块移位变换 P 可以不同. 显然,图 1 所示的四分组 CLEFIA 结构是图 2 所示的四分组类 CLEFIA 结构的特例.

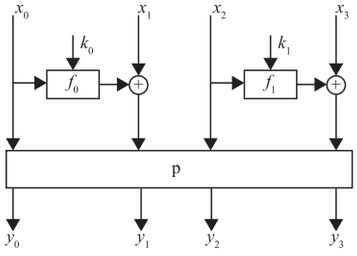

图2 四分组类CLEFIA结构

定义 1[6] 设 $f: Z_2^m \to Z_2^n$ 是多输出布尔函数,$\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_m) \in Z_2^m$,$\beta = (\beta_1, \beta_2, \cdots, \beta_n) \in Z_2^n$,记

$$\rho = \rho_f(\alpha \to \beta) = W_{(\beta f)}(\alpha) = \frac{1}{2^m} \sum_{x \in Z_2^m} (-1)^{\beta \cdot f(x) \oplus \alpha \cdot x},$$

则称 $\alpha \xrightarrow{\rho} \beta$ 为 f 的一个线性逼近. 其中,α 表示输入线性逼近,β 表示输出线性逼近,"$\alpha \cdot x$"表示点乘 $\alpha \cdot x = \alpha_0 x_0 \oplus \alpha_1 x_1 \oplus \cdots \oplus \alpha_{m-1} x_{m-1}$.

在本文中,有时为了方便,也将线性逼近 $\alpha \xrightarrow{\rho} \beta$ 简记为 $\alpha \to \beta$,并称 $\rho_f^2 = [\rho_f(\alpha \to \beta)]^2 = [\frac{1}{2^m} \sum_{x \in Z_2^m} (-1)^{\beta \cdot f(x) \oplus \alpha \cdot x}]^2$ 为线性逼近 $\alpha \to \beta$ 的概率.

显然,对四分组类 CLEFIA 结构,线性逼近(0,0,0,0)→(0,0,0,0)的概率恒为 1,此时,称(0,0,0,0)→(0,0,0,0)为平凡线性逼近,否则称为非平凡线性逼近. 以下只考虑非平凡的情形.

定义 2[7] 设 $\alpha \to \beta$ 是四分组类 CLEFIA 结构的轮函数(f_0 或 f_1)的一个线性逼近,若 $\beta \neq 0$,则称该轮函数是活动的.

引理 1[8] 对图 1 所示的四分组 CLEFIA 结构,设轮函数都是双射,则 $r(r \geq 1)$ 轮线性逼近至少有 $r - \lceil (r \bmod 6)/6 \rceil$ 个活动轮函数. 其中,$r \bmod 6$ 表示 r 除以 6 的最小非负余数,$\lceil x \rceil$ 表示不小于 x 的最小整数.

3 基于循环左移和循环右移变换的四分组类 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).

用 C^n 表示 $4n(n \geq 1)$ 轮四分组类 CLEFIA 结构. 其中,$G_1, G_2, \cdots, G_n$ 的含义如下: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,从而可将该结构分成 n 个"单元",即 $G_1, G_2, \cdots, G_n$. 于是,C^n 可表示成 $C^n = G_n \bullet G_{n-1} \bullet \cdots \bullet G_2 \bullet G_1$. 这里,"$\bullet$"表示变换的复合. 在同一个"单元" $G_i (1 \leq i \leq n)$ 内,每一轮中的块移位变换都是相同的,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. 顺便指出,这里的块移位变换之所以从循环左移变换和循环右移变换中选取,主要是考虑到实现的方便.

因任一"单元" $G_i (1 \leq i \leq n)$ 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,故基于循环左移和循环右移变换的四分组类 CLEFIA 结构共有 2^n 种,这 2^n 种结构共同构成一个变换簇,称为基于循环左移和循环右移变换的四分组类 CLEFIA 变换簇,简称四分组类 CLEFIA 变换簇,记作 $M^n = \{C^n \mid C^n = G_n \bullet G_{n-1} \bullet$

$\cdots \bullet G_2 \bullet G_1, P_i \in \{p_1, p_2\}, 1 \leqslant i \leqslant n\}$. 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 变换簇抵抗线性密码分析的实际安全性

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)(见图1),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)的线性逼近的结构形式;其次,利用所得到的线性逼近的结构形式,给出关于 CLEFIA-(2341)和 CLEFIA-(4123)的 2 轮线性逼近的两个引理;最后,利用这两个引理,给出四分组类 CLEFIA 变换簇抵抗线性密码分析的安全性评估结果.

首先给出四分组类 CLEFIA 结构 CLEFIA-(2341)和 CLEFIA-(4123)的线性逼近的结构形式.

定理 1　(1)对四分组类 CLEFIA 结构 CLEFIA-(2341)而言,圈函数 $Q_k(x_0, x_1, x_2, x_3) = (x_1 \oplus f_0(x_0 \oplus k_0), x_2, x_3 \oplus f_1(x_2 \oplus k_1), x_0)$ 的具有非零概率的线性逼近都具有形式

$$(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \rightarrow (\alpha_1, \alpha_2 \oplus \gamma_1, \alpha_3, \alpha_0 \oplus \gamma_0),$$

且轮函数 f_0 和 f_1 相应的线性逼近分别为 $\gamma_0 \rightarrow \alpha_1$ 和 $\gamma_1 \rightarrow \alpha_3$,并有

$$\rho^2_{Q_4}((\alpha_0, \alpha_1, \alpha_2, \alpha_3) \rightarrow (\alpha_1, \alpha_2 \oplus \gamma_1, \alpha_3, \alpha_0 \oplus \gamma_0)) = \rho^2_{f_0}(\gamma_0 \rightarrow \alpha_1) \cdot \rho^2_{f_1}(\gamma_1 \rightarrow \alpha_3).$$

(2)对四分组类 CLEFIA 结构 CLEFIA-(4123)而言,圈函数 $Q_k(x_0, x_1, x_2, x_3) = (x_3 \oplus f_1(x_2 \oplus k_1), x_0, x_1 \oplus f_0(x_0 \oplus k_0), x_2)$ 的具有非零概率的线性逼近都具有形式

$$(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \rightarrow (\alpha_3, \alpha_0 \oplus \gamma_0, \alpha_1, \alpha_2 \oplus \gamma_1),$$

且轮函数 f_0 和 f_1 相应的线性逼近分别为 $\gamma_0 \rightarrow \alpha_1$ 和 $\gamma_1 \rightarrow \alpha_3$,并有

$$\rho^2_{Q'_4}((\alpha_0, \alpha_1, \alpha_2, \alpha_3) \rightarrow (\alpha_3, \alpha_0 \oplus \gamma_0, \alpha_1, \alpha_2 \oplus \gamma_1)) = \rho^2_{f_0}(\gamma_0 \rightarrow \alpha_1) \cdot \rho^2_{f_1}(\gamma_1 \rightarrow \alpha_3).$$

证明　只证结论(1),结论(2)类似可证.

设 $(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \rightarrow (\beta_0, \beta_1, \beta_2, \beta_3)$ 是 $Q_k(x_0, x_1, x_2, x_3)$ 的具有非零概率的线性逼近,则

$$\begin{aligned}&(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \cdot (x_0, x_1, x_2, x_3) \oplus (\beta_0, \beta_1, \beta_2, \beta_3) \cdot Q_k(x_0, x_1, x_2, x_3)\\ &= \alpha_0 x_0 \oplus \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus \alpha_3 x_3 \oplus \beta_0(x_1 \oplus f_0(x_0 \oplus k_0)) \oplus \beta_1 x_2 \oplus \beta_2(x_3 \oplus f_1(x_2 \oplus k_1)) \oplus \beta_3 x_0\\ &= (\alpha_1 \oplus \beta_0) x_1 \oplus (\alpha_3 \oplus \beta_2) x_3 \oplus (\alpha_0 \oplus \beta_3) x_0 \oplus \beta_0 f_0(x_0 \oplus k_0) \oplus (\alpha_2 \oplus \beta_1) x_2 \oplus \beta_2 f_1(x_2 \oplus k_1) \quad (1)\end{aligned}$$

若 $\alpha_1 \oplus \beta_0$ 和 $\alpha_3 \oplus \beta_2$ 不全为零,则 $(\alpha_1 \oplus \beta_0) x_1 \oplus (\alpha_3 \oplus \beta_2) x_3$ 是平衡布尔函数,而 $(\alpha_1 \oplus \beta_0) x_1 \oplus (\alpha_3 \oplus \beta_2) x_3$ 与 $(\alpha_0 \oplus \beta_3) x_0 \oplus \beta_0 f_0(x_0 \oplus k_0) \oplus (\alpha_2 \oplus \beta_1) x_2 \oplus \beta_2 f_1(x_2 \oplus k_1)$ 独立,故 $(\alpha_1 \oplus \beta_0) x_1 \oplus (\alpha_3 \oplus \beta_2) x_3 \oplus (\alpha_0 \oplus \beta_3) x_0 \oplus \beta_0 f_0(x_0 \oplus k_0) \oplus (\alpha_2 \oplus \beta_1) x_2 \oplus \beta_2 f_1(x_2 \oplus k_1)$ 也是平衡布尔函数,也即 $(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \cdot (x_0, x_1, x_2, x_3) \oplus (\beta_0, \beta_1, \beta_2, \beta_3) \cdot Q_k(x_0, x_1, x_2, x_3)$ 是平衡布尔函数,这与条件"具有非零概率的线性逼近"矛盾,故 $\alpha_1 \oplus \beta_0 = \alpha_3 \oplus \beta_2 = 0$,即 $\beta_0 = \alpha_1$ 且 $\beta_2 = \alpha_3$,于是 $Q_k(x_0, x_1, x_2, x_3)$ 的具有非零概率的线性逼近都具有形式 $(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \rightarrow (\alpha_1, \beta_1, \alpha_3, \beta_3)$,此时,式(1)可进一步化简为 $(\alpha_0 \oplus \beta_3) x_0 \oplus \alpha_1 f_0(x_0 \oplus k_0) \oplus (\alpha_2 \oplus \beta_1) x_2 \oplus \alpha_3 f_1(x_2 \oplus k_1)$,从而轮函数 f_0 和 f_1 相应的线性逼近分别为 $\alpha_0 \oplus \beta_3 \rightarrow \alpha_1, \alpha_2 \oplus \beta_1 \rightarrow \alpha_3$.

令 $\alpha_0 \oplus \beta_3 = \gamma_0, \alpha_2 \oplus \beta_1 = \gamma_1$,则 $\beta_3 = \alpha_0 \oplus \gamma_0, \beta_1 = \alpha_2 \oplus \gamma_1$,从而 $(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \rightarrow (\alpha_1, \beta_1, \alpha_3, \beta_3)$ 就转化为 $(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \rightarrow (\alpha_1, \alpha_2 \oplus \gamma_1, \alpha_3, \alpha_0 \oplus \gamma_0)$,轮函数 f_0 和 f_1 相应的线性逼近 $\alpha_0 \oplus \beta_3 \rightarrow \alpha_1, \alpha_2 \oplus \beta_1 \rightarrow \alpha_3$ 就转化为 $\gamma_0 \rightarrow \alpha_1, \gamma_1 \rightarrow \alpha_3$. 其它结论显然,结论(1)成立. 证毕

其次,给出关于 CLEFIA-(2341)和 CLEFIA-(4123)的 2 轮线性逼近的两个引理.

在以下的分析中,假设轮函数 f_0 和 f_1 都是双射,并用 $\alpha \xrightarrow{R(v)} \beta$ 表示输入线性逼近为 α,输出线性逼近为 β 的 R 轮线性逼近,其中 $\alpha = (\alpha_0, \alpha_1, \alpha_2, \alpha_3), \beta = (\beta_0, \beta_1, \beta_2, \beta_3)$,$v$ 表示输入线性逼近 α 经过 R 轮迭代后,总共有 v 个轮函数是活动的. 因为在计算活动轮函数的个数时,并不需要考虑轮函数的具体结构,所以不妨设 CLEFIA-(2341)和 CLEFIA-(4123)中的轮函数都是相同的,并用"0"表示零线性逼近,"1"表示非零线性逼近,因此,非零线性逼近仅有 15 种表示:即 1 = (0,0,0,1),2 = (0,0,1,0),…,15 = (1,1,1,1).

利用上述的表示方法,设 CLEFIA-(2341)的轮函数的线性逼近为 $\alpha \rightarrow \beta$,CLEFIA-(4123)的轮函数的线性逼近为 $\xi \rightarrow \eta$,则由轮函数都是双射知,α 和 β 同时为零或同时不为零,ξ 和 η 同时为零或同时不为零,从而若有 $\alpha = \xi$,则有 $\beta = \eta$(注意,此时 α、β、ξ 和 η 只能为 0 或 1).

注意,按照上述的表示方法,"1"仅仅表示非零线性逼近,其具体值并不明确,在进行异或运算时遵循以下规则:$0 \oplus 0 = 0, 0 \oplus 1 = 1 \oplus 0 = 1, 1 \oplus 1 = 0$ 或 1,以下引理 2 证明过程中的线性逼近采用的都是上述的表示方法,且异或运算遵循上述的运算规则.

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,若 CLE-

FIA-(2341)存在线性逼近 $\alpha \xrightarrow{1(u)} \xi \xrightarrow{1(v)} \beta$,则 CLEFIA-(4123)存在线性逼近 $\alpha \xrightarrow{1(u)} \eta \xrightarrow{1(v)} \beta$ 与之对应,反之亦然;从而,若 CLEFIA-(2341)存在线性逼近 $\alpha \xrightarrow{2(s)} \beta$,则 CLEFIA-(4123)存在线性逼近 $\alpha \xrightarrow{2(s)} \beta$ 与之对应,反之亦然.

证明 设 CLEFIA-(2341)的输入线性逼近为 $\alpha=(\alpha_0,\alpha_1,\alpha_2,\alpha_3)$,则由定理 1(1)知,$\alpha$ 经过 2 轮迭代的线性逼近形式为

$$(\alpha_0,\alpha_1,\alpha_2,\alpha_3)\xrightarrow{1(u)}(\alpha_1,\alpha_2\oplus\gamma_1,\alpha_3,\alpha_0\oplus\gamma_0)\xrightarrow{1(v)}(\alpha_2\oplus\gamma_1,\alpha_3\oplus\gamma_3,\alpha_0\oplus\gamma_0,\alpha_1\oplus\gamma_2),$$

其中轮函数的线性逼近依次分别为 $\gamma_0\to\alpha_1,\gamma_1\to\alpha_3,\gamma_2\to\alpha_2\oplus\gamma_1,\gamma_3\to\alpha_0\oplus\gamma_0$,则 u 等于$\{\alpha_1,\alpha_3\}$中非零元素的个数,v 等于$\{\alpha_2\oplus\gamma_1,\alpha_0\oplus\gamma_0\}$中非零元素的个数.

将 α 作为 CLEFIA-(4123)的输入线性逼近,则由定理 1(2)知,α 经过 2 轮迭代的线性逼近形式为

$$(\alpha_0,\alpha_1,\alpha_2,\alpha_3)\xrightarrow{1(u')}(\alpha_3,\alpha_0\oplus\delta_0,\alpha_1,\alpha_2\oplus\delta_1)\xrightarrow{1(v')}(\alpha_2\oplus\delta_1,\alpha_3\oplus\delta_2,\alpha_0\oplus\delta_0,\alpha_1\oplus\delta_3),$$

其中轮函数的线性逼近依次分别为 $\delta_0\to\alpha_1,\delta_1\to\alpha_3,\delta_2\to\alpha_0\oplus\delta_0,\delta_3\to\alpha_2\oplus\delta_1$,则 u'等于$\{\alpha_1,\alpha_3\}$中非零元素的个数,v'等于$\{\alpha_0\oplus\delta_0,\alpha_2\oplus\delta_1\}$中非零元素的个数,显然 $u=u'$.

由线性逼近 $\gamma_0\to\alpha_1,\gamma_1\to\alpha_3,\delta_0\to\alpha_1,\delta_1\to\alpha_3$ 和轮函数都是双射以及上述记法知 $\gamma_0=\alpha_1,\gamma_1=\alpha_3,\delta_0=\alpha_1,\delta_1=\alpha_3$,从而 $\gamma_0=\delta_0,\gamma_1=\delta_1$,于是 $\alpha_0\oplus\gamma_0=\alpha_0\oplus\delta_0,\alpha_2\oplus\gamma_1=\alpha_2\oplus\delta_1$,故 $v=v'$. 由线性逼近 $\gamma_2\to\alpha_2\oplus\gamma_1,\gamma_3\to\alpha_0\oplus\gamma_0,\delta_2\to\alpha_0\oplus\delta_0,\delta_3\to\alpha_2\oplus\delta_1$ 和轮函数都是双射以及上述记法知 $\gamma_2=\alpha_2\oplus\gamma_1,\gamma_3=\alpha_0\oplus\gamma_0,\delta_2=\alpha_0\oplus\delta_0,\delta_3=\alpha_2\oplus\delta_1$,而前面已证明 $\gamma_0=\delta_0,\gamma_1=\delta_1$,从而 $\gamma_3=\delta_2,\gamma_2=\delta_3$,于是 $\alpha_3\oplus\gamma_3=\alpha_3\oplus\delta_2,\alpha_1\oplus\gamma_2=\alpha_1\oplus\delta_3$,再结合前面已证明的 $\alpha_0\oplus\gamma_0=\alpha_0\oplus\delta_0,\alpha_2\oplus\gamma_1=\alpha_2\oplus\delta_1$ 知

$$(\alpha_2\oplus\gamma_1,\alpha_3\oplus\gamma_3,\alpha_0\oplus\gamma_0,\alpha_1\oplus\gamma_2)=(\alpha_2\oplus\delta_1,\alpha_3\oplus\delta_2,\alpha_0\oplus\delta_0,\alpha_1\oplus\delta_3).$$

这样就证明了:若 CLEFIA-(2341)存在线性逼近

$$(\alpha_0,\alpha_1,\alpha_2,\alpha_3)\xrightarrow{1(u)}(\alpha_1,\alpha_2\oplus\gamma_1,\alpha_3,\alpha_0\oplus\gamma_0)\xrightarrow{1(v)}(\alpha_2\oplus\delta_1,\alpha_3\oplus\delta_2,\alpha_0\oplus\delta_0,\alpha_1\oplus\delta_3),$$

则 CLEFIA-(4123)存在线性逼近

$$(\alpha_0,\alpha_1,\alpha_2,\alpha_3)\xrightarrow{1(u')}(\alpha_3,\alpha_0\oplus\delta_0,\alpha_1,\alpha_2\oplus\delta_1)\xrightarrow{1(v')}(\alpha_2\oplus\delta_1,\alpha_3\oplus\delta_2,\alpha_0\oplus\delta_0,\alpha_1\oplus\delta_3).$$

记

$$\xi=(\alpha_1,\alpha_2\oplus\gamma_1,\alpha_3,\alpha_0\oplus\gamma_0),$$

$$\eta=(\alpha_3,\alpha_0\oplus\delta_0,\alpha_1,\alpha_2\oplus\delta_1),$$

$$\beta=(\alpha_2\oplus\gamma_1,\alpha_3\oplus\gamma_3,\alpha_0\oplus\gamma_0,\alpha_1\oplus\gamma_2)=(\alpha_2\oplus\delta_1,\alpha_3\oplus\delta_2,\alpha_0\oplus\delta_0,\alpha_1\oplus\delta_3),$$

则上面已证明的结论就是:若 CLEFIA-(2341)存在线性逼近 $\alpha \xrightarrow{1(u)} \xi \xrightarrow{1(v)} \beta$,则 CLEFIA-(4123)存在线性逼近 $\alpha \xrightarrow{1(u)} \eta \xrightarrow{1(v)} \beta$ 与之对应.

反之,同理可证:若 CLEFIA-(4123)存在线性逼近 $\alpha \xrightarrow{1(u)} \eta \xrightarrow{1(v)} \beta$,则 CLEFIA-(2341)存在线性逼近 $\alpha \xrightarrow{1(u)} \xi \xrightarrow{1(v)} \beta$ 与之对应.

记 $s=u+v$,线性逼近 $\alpha \xrightarrow{1(v)} \xi \xrightarrow{1(v)} \beta$ 和 $\alpha \xrightarrow{1(v)} \eta \xrightarrow{1(v)} \beta$ 都可以记为 $\alpha \xrightarrow{2(s)} \beta$ 的形式,本引理结论成立. 证毕

引理 2 实际上是说:CLEFIA-(2341)存在 2 轮线性逼近 $\alpha \xrightarrow{2(s)} \beta$ 当且仅当 CLEFIA-(4123)存在 2 轮线性逼近 $\alpha \xrightarrow{2(s)} \beta$.

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,且设 $\alpha \xrightarrow{1(u)} \delta(\alpha\neq 0)$ 是 CLEFIA-(2341)的 1 轮线性逼近,$\alpha \xrightarrow{1(s)} \xi(\alpha\neq 0)$ 是 CLEFIA-(4123)的 1 轮线性逼近,则 $u=s$.

证明 由定理 1,设$(\alpha_0,\alpha_1,\alpha_2,\alpha_3)\to(\alpha_1,\alpha_2\oplus\gamma_1,\alpha_3,\alpha_0\oplus\gamma_0)$是四分组类 CLEFIA 结构 CLEFIA-(2341)的 1 轮线性逼近,$(\alpha_0,\alpha_1,\alpha_2,\alpha_3)\to(\alpha_3,\alpha_0\oplus\gamma_0,\alpha_1,\alpha_2\oplus\gamma_1)$是 CLEFIA-(2341)的 1 轮线性逼近,则 u 和 v 都等于$\{\alpha_1,\alpha_3\}$中非零元素的个数,本引理结论成立. 证毕

引理 3 实际上是说:若 CLEFIA-(2341)和 CLEFIA-(4123)的 1 轮线性逼近的非零输入线性逼近相同,则活动轮函数的个数也相同,即 $u=s$.

由引理 2、引理 3 可得如下定理.

定理 2 设 M^n 是基于循环左移和循环右移变换的四分组类 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 $r(1\leqslant r\leqslant 4n)$轮线性逼近至少有 $r-\lceil(r\bmod 6)/6\rceil$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,$\lceil x\rceil$表示不小于 x 的最小整数.

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

由引理 1 知,要想证明本定理结论成立,只需证明 C^n 的 r 轮线性逼近与 CLEFIA-(2341)的 r 轮线性逼近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 轮线性逼近当且

仅当 C^n 也存在一条具有同样多个活动轮函数的 r 轮线性逼近.

下面根据线性逼近的轮数 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 2 知,CLEFIA-(2341)存在 2 轮线性逼近 $\alpha\xrightarrow{2(u)}\beta$ 当且仅当 CLEFIA-(4123)也存在线性逼近 $\alpha\xrightarrow{2(u)}\beta$,从而,由 C^n 的含义知,CLEFIA-(2341)存在 r 轮线性逼近 $\alpha_1\xrightarrow{2(u_1)}\alpha_2\xrightarrow{2(u_2)}\alpha_3\xrightarrow{2(u_3)}\cdots\xrightarrow{2(u_{k-1})}\alpha_k\xrightarrow{2(u_k)}\alpha_{k+1}$当且仅当 C^n 也存在 r 轮线性逼近 $\alpha_1\xrightarrow{2(u_1)}\alpha_2\xrightarrow{2(u_2)}\alpha_3\xrightarrow{2(u_3)}\cdots\xrightarrow{2(u_{k-1})}\alpha_k\xrightarrow{2(u_k)}\alpha_{k+1}$,其中 $k=r/2$. 从而,C^n 的 r 轮线性逼近与 CLEFIA-(2341)的 r 轮线性逼近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 $r-1$ 轮线性逼近 $\alpha_1\xrightarrow{2(u_1)}\alpha_2\xrightarrow{2(u_2)}\alpha_3\xrightarrow{2(u_3)}\cdots\xrightarrow{2(u_{k-1})}\alpha_k\xrightarrow{2(u_k)}\alpha_{k+1}$当且仅当 C^n 也存在 $r-1$ 轮线性逼近 $\alpha_1\xrightarrow{2(u_1)}\alpha_2\xrightarrow{2(u_2)}\alpha_3\xrightarrow{2(u_3)}\cdots\xrightarrow{2(u_{k-1})}\alpha_k\xrightarrow{2(u_k)}\alpha_{k+1}$,其中 $k=(r-1)/2$.

再设 $\alpha_{k+1}\xrightarrow{1(v)}\alpha_{k+2}(v\geq 0)$是 CLEFIA-(2341)的 1 轮线性逼近,$\alpha_{k+1}\xrightarrow{1(s)}\xi(s\geq 0)$是 CLEFIA-(4123)的 1 轮线性逼近(注:由引理 3 知 $v=s$),则由 C^n 的含义知,CLEFIA-(2341)存在 r 轮线性逼近 $\alpha_1\xrightarrow{2(u_1)}\alpha_2\xrightarrow{2(u_2)}\alpha_3\xrightarrow{2(u_3)}\cdots\xrightarrow{2(u_{k-1})}\alpha_k\xrightarrow{2(u_k)}\alpha_{k+1}\xrightarrow{1(v)}\alpha_{k+2}$当且仅当以下两个条件之一成立.

(A) C^n 存在 r 轮线性逼近 $\alpha_1\xrightarrow{2(u_1)}\alpha_2\xrightarrow{2(u_2)}\alpha_3\xrightarrow{2(u_3)}\cdots\xrightarrow{2(u_{k-1})}\alpha_k\xrightarrow{2(u_k)}\alpha_{k+1}\xrightarrow{1(v)}\alpha_{k+2}$.

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

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3 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 轮线性逼近当且仅当 C^n 也存在一条具有同样多个活动轮函数的 r 轮线性逼近,从而 C^n 的 r 轮线性逼近与 CLEFIA-(2341)的 r 轮线性逼近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 轮线性逼近与 CLEFIA-(2341)的 r 轮线性逼近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 2 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)分组密码结构抵抗线性密码分析的安全性评估结果. 不难看出,定理 2 的证明主要是利用了四分组类 CLEFIA 结构 CLEFIA-(2341)和 CLEFIA-(4123)的线性逼近之间的关系.

由定理 2 立得以下定理 3.

定理 3　设 M^n 是基于循环左移和循环右移变换的四分组类 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线性逼近概率为 $q_{\max}$,则 C^n 的 $r(1\leqslant r\leqslant 4n)$轮线性逼近概率$\leqslant[q_{\max}]^{r-\lceil(r\bmod 6)/6\rceil}$.

5　需进一步探讨的若干问题

本文提出了四分组类 CLEFIA 变换簇,现在有以下两个问题需要进一步探讨.

问题 1:将四分组类 CLEFIA 结构中的循环左移变换和循环右移变换替换成其它的两个不同的块移位变换时,未必有类似于定理 2 的结论成立,那么,这两个不同的块移位变换满足什么样的条件时,才有类似于定理 2 的结论成立?

问题 2:类似于四分组类 CLEFIA 变换簇,可以定义 $m(m\geqslant 4)$分组类 CLEFIA 变换簇,那么,对于一般的 m 分组类 CLEFIA 变换簇,是否也有类似于定理 2 的结论成立?这里所说的 m 分组,是指将输入分成 m 个分块的情形.

6　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线性逼近之间的关系,给出了变换簇中所有密码结构(而不仅仅是一种)抵抗线性密码分析的安全性评估结果. 这种利用变换簇对分组密码进行研究的方法,为分组密码的安全性评估提供了一个较为新颖的思路. 在此基础上,本文提出需要进一步探讨的若干问题. 目前,这些问题正在逐步解决中.

参考文献

[1] Mitsuru Matsui. Linear cryptanalysis method for DES cipher[A]. Proceedings of Advances in Cryptology-EUROCRYPT'93[C]. LNCS 765, Berlin Heidelberg: Springer-Verlag, 1994. 386 – 397.

[2] 吴文玲,冯登国,张文涛. 分组密码的设计与分析[M]. 北京:清华大学出版社,2009.
Wu Wenling, Feng Dengguo, Zhang Wentao. Design and Analysis of Block Cipher[M]. Beijing: Tsinghua University Press, 2009. (in Chinese)

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

[4] 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)

[5] 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.

[6] 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 Chenhui, Zheng Haoran, Zhang Shaowu, et al. Cryptology[M]. Beijing: Higher Education Press, 2009. (in Chinese)

[7] Bruce Schneier, John Kelsey. Unbalanced Feistel networks and block cipher design[A]. Proceedings of Fast Software Encryption-FSE'96[C]. LNCS1039, Cambridge: Springer-Verlag, 1996. 121 – 144.

[8] 王健康. 几类分组密码模型的安全性分析[D]. 解放军信息工程大学硕士学位论文,2013.
Wang Jiankang. Security analysis of several block cipher models[D]. the PLA Information Engineering University, 2013. (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