两类动态密码结构抵抗不可能差分和零相关线性能力评估

沈 璇[1],刘国强[2,3*],孙 兵[2,4],何 俊[1]

(1. 国防科技大学信息通信学院,湖北武汉 430010;2. 国防科技大学理学院,湖南长沙 410073;3. 中国科学院信息工程研究所,信息安全国家重点实验室,北京 100093;4. 商用密码理论与技术创新湖南省工程研究中心,湖南长沙 410000)

摘 要: 动态密码的设计与分析是当前密码学领域研究的热点. 本文针对类CLEFIA动态密码结构和四分组CLEFIA变换簇抵抗不可能差分和零相关线性分析的能力进行评估. 当两类动态密码结构的轮函数为双射时,通过研究密码组件的可交换性质,证明了这两类动态密码结构各自置换等价于标准静态密码结构. 利用建立的置换等价关系,通过构造静态密码结构不可能差分和零相关线性区分器,证明了4n轮类CLEFIA动态密码结构所有结构均存在8轮的不可能差分和零相关线性区分器,证明了4n轮四分组CLEFIA变换簇所有结构均存在9轮的不可能差分和零相关线性区分器.

关键词: 分组密码;动态密码;类CLEFIA动态密码结构;四分组CLEFIA变换簇;不可能差分;零相关线性

基金项目: 国家自然科学基金(No.62002370, No.62272470, No.61702537);国防科技大学科研计划项目(No. ZK21-36);信息安全国家重点实验室开放基金(No.2020-MS-02)

中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112(2024)03-0709-10

电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20220311

Security Evaluation Against Impossible Differential Cryptanalysis and Zero Correlation Linear Cryptanalysis for Two Dynamic Cryptographic Structures

SHEN Xuan[1], LIU Guo-qiang[2,3*], SUN Bing[2,4], HE Jun[1]

(1. *College of Information and Communication*, *National University of Defense Technology*, *Wuhan*, *Hubei* 430010, *China*;
2. *College of Sciences*, *National University of Defense Technology*, *Changsha*, *Hunan* 410073, *China*;
3. *State Key Laboratory of Information Security*, *Institute of Information Engineering*, *Chinese Academy of Sciences*, *Beijing* 100093, *China*;
4. *Hunan Engineering Research Center of Commercial Cryptography Theory and Technology Innovation*, *Changsha*, *Hunan* 410000, *China*)

Abstract: The design and analysis of dynamic block ciphers are the frontier of current cryptography research. For CLEFIA-like dynamic cryptographic structure and four-block CLEFIA-like transform cluster, this paper focuses on the security evaluation against impossible differential cryptanalysis and zero correlation linear cryptanalysis. When the round functions of the two dynamic cryptographic structures are bijective, by studying the commutative properties of the modules, the fact that the two dynamic cryptographic structures are permutation equivalence of the two static structures respectively can be proved. With the established equivalence relation, by constructing the impossible differential and zero correlation distinguishers of two static structures, 8-round impossible differentials and zero correlation linear hulls of 4n-round CLEFIA-like dynamic cryptographic structure can be found as well 9-round ones for 4n-round four-block CLEFIA-like transform cluster.

Key words: block cipher; dynamic cryptographic structure; CLEFIA-like dynamic cryptographic structure; four-block CLEFIA-like transform cluster; impossible differentials; zero correlation linear hulls

Foundation Item(s): National Natural Science Foundation of China (No.62002370, No.62272470, No.61702537);

收稿日期:2022-03-25;修回日期:2022-08-03;责任编辑:梅志强

*通讯作者:刘国强

Scientific Research Plan of National University of Defense Technology (No.ZK21-36); State Key Laboratory of Information Security (No.2020-MS-02)

1 引言

随着信息技术的飞速发展,蕴含各类敏感信息的海量数据正在加速形成. 核心数据的安全性至关重要,而确保数据安全最重要的手段之一是利用分组密码对重要数据进行保护. 国内外分组密码标准算法有很多,如 AES (Advanced Encyption Standard)[1] 、SM4[2] 、CLEFIA[3]等,但这些标准算法均是静态的,即算法结构和组件均是固定的. 随着信息交互的愈加频繁,信息处理的要求也随之提高,现有分组密码并不能完全满足相应的要求,这需要创新密码设计理论. 在这一背景下,许多密码学者提出了动态分组密码的设计理念. 动态分组密码需要包含足够多的分组密码实例,同时加解密安全强度需要保持近似一致. 目前动态分组密码的设计主要利用各种参数来控制密码结构或组件的动态变化. 例如,密码学界提出了一种可调分组密码[4],相比传统分组密码,可调分组密码通过引入公开参数来控制密码算法的动态变化,极大地提高了密码算法的可变性. 此外,还有一种构造动态密码结构的思路:将静态分组密码的部分结构或组件动态化,包括非线性组件 S 盒的动态化设计[5~7]、密码结构动态化设计[8~10]等.

在密码结构动态化设计方面,2017 年,王念平[11]基于 CLEFIA 密码结构,通过控制块移位操作的选取,设计了“四分组类 CLEFIA 变换簇”的动态密码结构,该结构 $4n$ 轮蕴含的所有不同密码结构的数量为 2^n. 进一步,在轮函数为双射的条件下,王念平利用该动态密码结构中两种特殊密码结构的差分对应和线性对应关系,分别给出了该动态密码结构中所有结构抵抗差分密码分析[11]和线性密码分析[12]的安全性评估结果. 2021 年,杨继林等人[13]借鉴四分组类 CLEFIA 变换簇设计思想,通过改变部分轮的线性层,推广设计了类 CLEFIA 动态密码结构,该结构 $4n$ 轮蕴含的所有不同密码结构的数量为 2^{4n}. 进一步,在轮函数为双射的条件下,他们通过建立类 CLEFIA 动态密码结构中两类不同密码结构的差分对应关系,给出了类 CLEFIA 动态密码结构的差分密码分析结果.

本文主要研究上述两种动态密码结构抵抗不可能差分和零相关线性分析的能力. 同样地,在轮函数为双射的前提条件下,根据构造不可能差分和零相关线性区分器的特点,首先给出这两类动态密码结构的等价表示. 其次,通过挖掘密码组件的可交换性质,证明了 $4n$ 轮类 CLEFIA 动态密码结构置换等价于标准静态密码结构. 通过构造该标准静态密码结构的 8 轮不可能差分和零相关线性区分器,利用构造的置换等价关系,证明了 $4n$ 轮类 CLEFIA 动态密码结构均存在 8 轮的不可能差分和零相关线性区分器. 最后,考虑到四分组类 CLEFIA 变换簇是类 CLEFIA 动态密码结构的简化版本,利用相同的思路,还证明了四分组类 CLEFIA 变换簇均存在 9 轮的不可能差分和零相关线性区分器. 具体结果比较如表 1 所示.

表 1 两类 $4n$ 轮动态密码结构的安全性评估结果

动态密码结构	密码分析方法	总轮数	活跃轮函数个数/区分器轮数	来源
类 CLEFIA 动态密码结构	差分分析	$r(1\leqslant r\leqslant 4n)$	$\geqslant r-1$	文献[13]
	不可能差分分析	$4n$	8	本文
	零相关线性分析	$4n$	8	本文
四分组类 CLEFIA 变换簇	差分分析	$r(1\leqslant r\leqslant 4n)$	$\geqslant r-\lfloor(r \bmod 6)/6\rfloor$	文献[11]
	线性分析	$r(1\leqslant r\leqslant 4n)$	$\geqslant r-\lfloor(r \bmod 6)/6\rfloor$	文献[12]
	不可能差分分析	$4n$	9	本文
	零相关线性分析	$4n$	9	本文

2 预备知识

2.1 类 CLEFIA 密码结构及其变体

图 1 为类 CLEFIA 密码结构. 它的轮迭代中有 2 个轮函数 f_0 和 f_1,它们均为非线性函数,在本文中,均视为双射函数. 此外,块移位变换 P 是循环左移或者循环右移变换,即 $P(\boldsymbol{x}_0, \boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3)=(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{x}_0)$ 或者 $P(\boldsymbol{x}_0, \boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3)=(\boldsymbol{x}_3, \boldsymbol{x}_0, \boldsymbol{x}_1, \boldsymbol{x}_2)$. 当块移位变换 P 为循环左移变换时与 CLEFIA 密码结构相同. 与类 CLEFIA 密码结构类似,它的变体结构在块移位变换 P 后增加了两个异或运算,如图 2 所示.

2.2 类 CLEFIA 动态密码结构

2021 年,杨继林等人在文献[13]中提出了 $4n(n\geqslant 1)$ 轮类 CLEFIA 动态密码结构(用 C^n 表示,下文中简称动态密码结构 C^n),如图 3 所示.

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 $G_i(1\leqslant i\leqslant n)$ 表示第 $4i-3$ 轮到第 $4i$ 轮,则

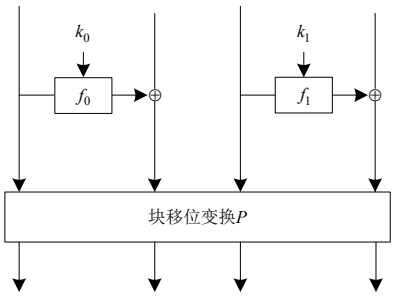


图1　类CLEFIA密码结构

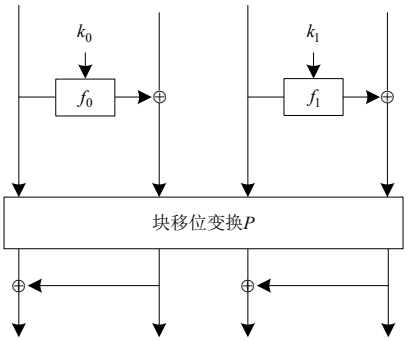


图2　类CLEFIA密码结构的变体

C^n可表示成:

$$C^n = G_n \cdot G_{n-1} \cdot \cdots \cdot G_2 \cdot G_1 \tag{1}$$

这里"·"表示变换的复合,在不影响上下文意思时可省略. 每一个单元$G_i(1\leqslant i\leqslant n)$由4轮变换组成,其中前3轮是类CLEFIA密码结构,最后1轮是类CLEFIA密码结构的变体. 在这4轮变换中,每轮变换的块移位操作均有2种选择,即循环左移1个块操作或者循环右移1个块操作(下文中简称循环左移或者循环右移). 故$4n$轮的动态密码结构C^n包含2^{4n}个不同的密码结构.

2.3　四分组类CLEFIA变换簇

2017年,王念平在文献[11]中设计了$4n(n\geqslant 1)$轮"四分组类CLEFIA变换簇"(用L^n表示,下文中简称动态密码结构L^n),如图4所示. 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$H_i(1\leqslant i\leqslant n)$表示第$4i-3$轮到第$4i$轮,从而$L^n$可表示成:

$$L^n = H_n \cdot H_{n-1} \cdot \cdots \cdot H_2 \cdot H_1 \tag{2}$$

在四分组类CLEFIA变换簇中,每个单元$H_i(1\leqslant i\leqslant n)$的4轮变换均为类CLEFIA密码结构,并且每轮的循环移位选择需相同,4轮同时为循环左移或者同时为循环右移. 但是在不同单元中循环移位选择不定,可以相同或不同. 故$4n$轮的四分组类CLEFIA变换簇包含2^n个不同的密码结构. 考虑到四分组类CLEFIA变换簇是动态密码结构C^n的简化版本,因此本文主要研究动态密码结构C^n,同时将相应的结论推广应用到四分组类CLEFIA变换簇中.

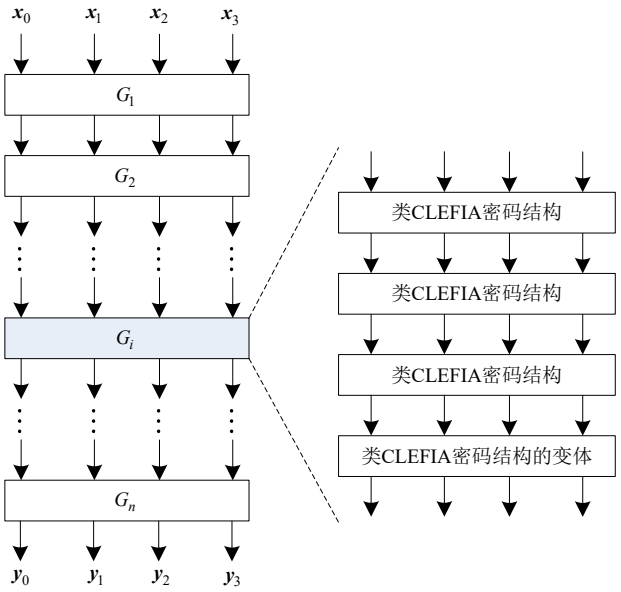


图3　类CLEFIA动态密码结构C^n

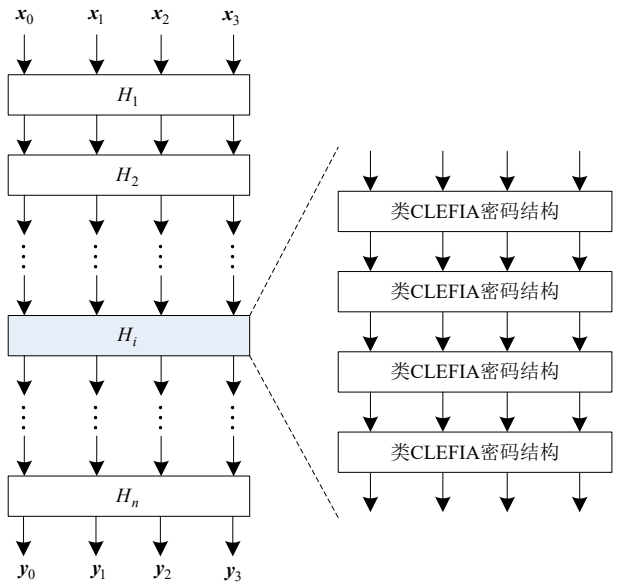


图4　四分组类CLEFIA变换簇L^n

2.4　不可能差分和零相关线性分析

不可能差分分析是由Knudsen[14]和Biham等人[15]独立提出,它是差分分析的一种变体,是目前分组密码安全性评估最重要的方法之一. 与差分分析利用高概率差分特征来恢复正确密钥不同,不可能差分分析主要是利用概率为0的差分来排除错误密钥. 与不可能差分分析类似,零相关线性分析[16]也是通过构造概率为0的线性壳来恢复密钥. 不可能差分和零相关线性

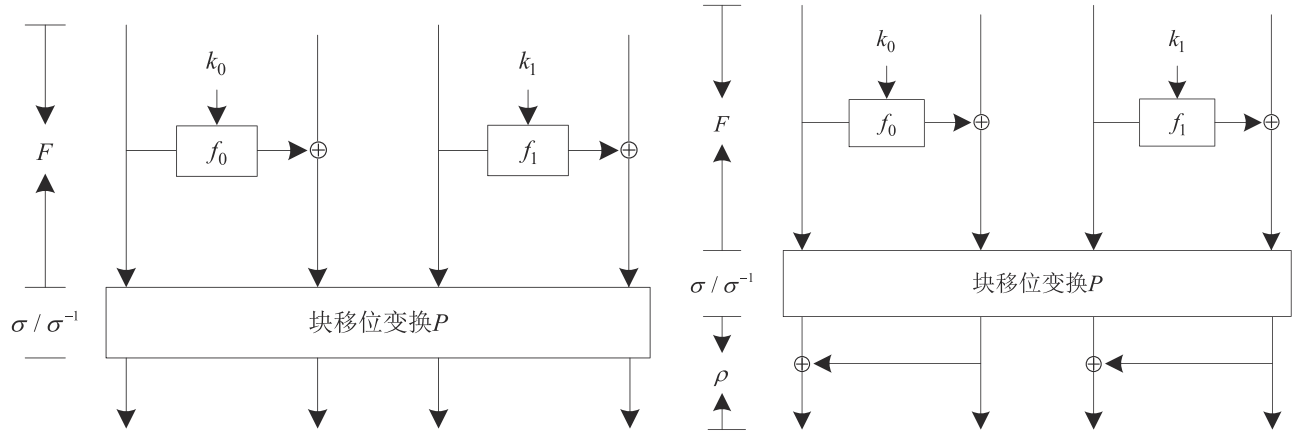
分析的核心是构造尽可能长的区分器. 目前构造这两类区分器最常用的方法是利用中间相错技术来实现. 该技术的思路是:当输入差分/掩码为$\boldsymbol{\alpha}$,以概率1正向加密传播r_0轮后,得到中间差分/掩码为$\boldsymbol{\gamma}_1$;同时,当输出差分/掩码为$\boldsymbol{\beta}$,以概率1反向解密传播r_1轮后,得到中间差分/掩码为$\boldsymbol{\gamma}_2$. 若$\boldsymbol{\gamma}_1\neq\boldsymbol{\gamma}_2$,则$\boldsymbol{\alpha}\to\boldsymbol{\beta}$是一条$r_0+r_1$轮的不可能差分/零相关线性区分器.

上述两种区分器在构造时,最常构造的是截断形式的区分器,即不考虑非线性组件的具体细节,仅将其视为双射函数. 对本文研究的两类动态密码结构而言,轮函数是其唯一的非线性组件,故在构造这两种区分器的时候也不考虑轮函数的细节,即仅考虑轮函数的双射性质:当输入差分/掩码为0时,经过轮函数后输出差分/掩码也为0;当输入差分/掩码非0时,经过轮函数后输出差分/掩码也非0. 此外,轮密钥是以异或方式参与加解密运算,不影响截断差分和线性传播. 因此,在研究动态密码结构的截断差分和线性传播规律时,可以直接忽略轮密钥.

3 动态密码结构的等价分类

3.1 类CLEFIA密码结构及其变体的等价表示

类CLEFIA密码结构及其变体如图1和图2所示. 当研究概率为1的截断差分和线性传播时,由于轮函数f_0和f_1只看成双射函数,故f_0和f_1是否相同不影响截断差分和线性传播规律. 因此,当轮函数f_0和f_1均视为f函数,不加以区分时,能够得到如图5所示类CLEFIA密码结构及其变体的等价表示. 显然,类CLEFIA密码结构及其变体与它们各自的等价表示之间具有相同的截断差分和线性传播规律. 特别地,在本文中,定义两个变换A和B相互等价"$A\sim B$",它是指变换A和变换B在轮函数为双射时具有相同的截断差分和线性传播规律. 进一步,在本文中,变换A的等价表示$\overline{A}$指的是将变换A中所有的轮函数均视为相同的轮函数f,其余组件均相同.



(a) 类CLEFIA密码结构的等价表示　　(b) 类CLEFIA密码结构变体的等价表示

图5 类CLEFIA密码结构及其变体的等价表示

在图5(a)中,类CLEFIA密码结构的等价表示由两部分变换组成:

(1)F变换:若输入和输出分别为$\boldsymbol{x}=(\boldsymbol{x}_0,\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3)$和$\boldsymbol{y}=(\boldsymbol{y}_0,\boldsymbol{y}_1,\boldsymbol{y}_2,\boldsymbol{y}_3)$,则有

$$\begin{aligned}\boldsymbol{y}=F(\boldsymbol{x})\Leftrightarrow&(\boldsymbol{y}_0,\boldsymbol{y}_1,\boldsymbol{y}_2,\boldsymbol{y}_3)\\=&(\boldsymbol{x}_0,f(\boldsymbol{x}_0)\oplus\boldsymbol{x}_1,\boldsymbol{x}_2,f(\boldsymbol{x}_2)\oplus\boldsymbol{x}_3)\end{aligned}\tag{3}$$

(2)σ/σ^{-1}变换:当块移位变换为循环左移变换和循环右移变换时,分别记为σ变换和σ^{-1}变换,也即$\sigma(\boldsymbol{x}_0,\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3)=(\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3,\boldsymbol{x}_0)$和$\sigma^{-1}(\boldsymbol{x}_0,\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3)=(\boldsymbol{x}_3,\boldsymbol{x}_0,\boldsymbol{x}_1,\boldsymbol{x}_2)$. 根据$\sigma$变换的定义可知:

$$\sigma^4=I,\ \sigma^{-1}=\sigma^3=\sigma^2\cdot\sigma\tag{4}$$

这里I变换表示恒等变换,即

$$I(\boldsymbol{x}_0,\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3)=(\boldsymbol{x}_0,\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3)\tag{5}$$

在图5(b)中,类CLEFIA密码结构变体的等价表示由三部分变换组成,其中F变换和σ/σ^{-1}变换与图5(a)定义相同,此外还有ρ变换,其定义如下:

若输入和输出分别为$\boldsymbol{x}=(\boldsymbol{x}_0,\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3)$和$\boldsymbol{y}=(\boldsymbol{y}_0,\boldsymbol{y}_1,\boldsymbol{y}_2,\boldsymbol{y}_3)$,则有

$$\boldsymbol{y}=\rho(\boldsymbol{x})\Leftrightarrow(\boldsymbol{y}_0,\boldsymbol{y}_1,\boldsymbol{y}_2,\boldsymbol{y}_3)=(\boldsymbol{x}_0\oplus\boldsymbol{x}_1,\boldsymbol{x}_1,\boldsymbol{x}_2\oplus\boldsymbol{x}_3,\boldsymbol{x}_3)\tag{6}$$

对于类CLEFIA动态密码结构C^n,第i个单元G_i($1\leqslant i\leqslant n$)可以等价表示为$\overline{G_i}$:

$$G_i\sim\overline{G_i}=(\rho\sigma^{j_0}F)\cdot(\sigma^{j_1}F)\cdot(\sigma^{j_2}F)\cdot(\sigma^{j_3}F)\tag{7}$$

这里$j_0,j_1,j_2,j_3\in\{1,-1\}$.

对于四分组类CLEFIA变换簇L^n,第i个单元H_i($1\leqslant i$

$\leqslant n$)可以等价表示为$\overline{H_i}$:

$$H_i \sim \overline{H_i} = (\sigma^m F)\cdot(\sigma^m F)\cdot(\sigma^m F)\cdot(\sigma^m F) \tag{8}$$

这里$m \in \{1,-1\}$. 显然,单元$\overline{H_i}$是$\overline{G_i}$的简化版本.

3.2　几类变换的可交换性质

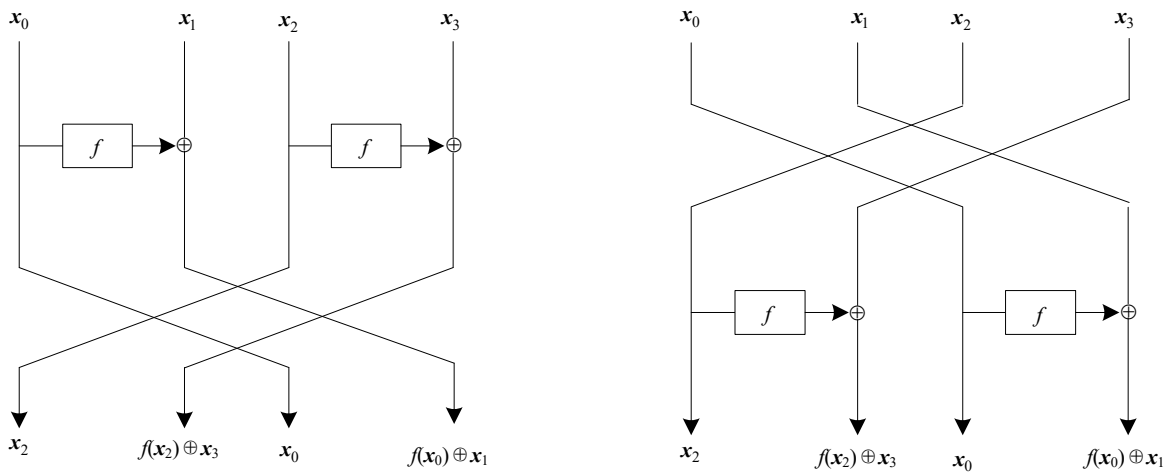
针对上节中的F变换、σ变换和ρ变换,给出如下两个引理:

引理1　σ^2变换和F变换满足可交换性质,即$\sigma^2 \cdot F = F \cdot \sigma^2$.

证明　如图6所示,σ变换表示循环左移1个块,σ^2变换表示循环左移2个块,若输入为$\boldsymbol{x}=(\boldsymbol{x}_0,\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3)$,则有$\sigma^2(\boldsymbol{x}_0,\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3)=(\boldsymbol{x}_2,\boldsymbol{x}_3,\boldsymbol{x}_0,\boldsymbol{x}_1)$. 下面分别计算$\sigma^2 \cdot F(\boldsymbol{x})$和$F \cdot \sigma^2(\boldsymbol{x})$:

$$\begin{cases} \sigma^2 \cdot F(\boldsymbol{x}) = \sigma^2\left[F(\boldsymbol{x})\right] \\ \qquad = \sigma^2\left(\boldsymbol{x}_0, f(\boldsymbol{x}_0)\oplus\boldsymbol{x}_1, \boldsymbol{x}_2, f(\boldsymbol{x}_2)\oplus\boldsymbol{x}_3\right) \\ \qquad = \left(\boldsymbol{x}_2, f(\boldsymbol{x}_2)\oplus\boldsymbol{x}_3, \boldsymbol{x}_0, f(\boldsymbol{x}_0)\oplus\boldsymbol{x}_1\right) \\ F \cdot \sigma^2(\boldsymbol{x}) = F\left[\sigma^2(\boldsymbol{x})\right] \\ \qquad = F\left(\boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{x}_0, \boldsymbol{x}_1\right) \\ \qquad = \left(\boldsymbol{x}_2, f(\boldsymbol{x}_2)\oplus\boldsymbol{x}_3, \boldsymbol{x}_0, f(\boldsymbol{x}_0)\oplus\boldsymbol{x}_1\right) \end{cases} \tag{9}$$

故对于任意的输入$\boldsymbol{x}$,$\sigma^2 \cdot F(\boldsymbol{x}) = F \cdot \sigma^2(\boldsymbol{x})$. 因此,$\sigma^2 \cdot F = F \cdot \sigma^2$. 引理得证.



(a) $\sigma^2 \cdot F$　　(b) $F \cdot \sigma^2$

图6　F变换和σ^2变换的先后复合

引理2　σ^2变换和ρ变换满足可交换性质,即$\sigma^2 \cdot \rho = \rho \cdot \sigma^2$

证明　如图7所示,若输入为$\boldsymbol{x}=(\boldsymbol{x}_0,\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3)$,则有

$$\begin{cases} \sigma^2 \cdot \rho(\boldsymbol{x}) = \sigma^2\left[\rho(\boldsymbol{x})\right] \\ \qquad = \sigma^2\left(\boldsymbol{x}_0\oplus\boldsymbol{x}_1, \boldsymbol{x}_1, \boldsymbol{x}_2\oplus\boldsymbol{x}_3, \boldsymbol{x}_3\right) \\ \qquad = \left(\boldsymbol{x}_2\oplus\boldsymbol{x}_3, \boldsymbol{x}_3, \boldsymbol{x}_0\oplus\boldsymbol{x}_1, \boldsymbol{x}_1\right) \\ \rho \cdot \sigma^2(\boldsymbol{x}) = \rho\left[\sigma^2(\boldsymbol{x})\right] \\ \qquad = \rho\left(\boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{x}_0, \boldsymbol{x}_1\right) \\ \qquad = \left(\boldsymbol{x}_2\oplus\boldsymbol{x}_3, \boldsymbol{x}_3, \boldsymbol{x}_0\oplus\boldsymbol{x}_1, \boldsymbol{x}_1\right) \end{cases} \tag{10}$$

故对于任意的输入$\boldsymbol{x}$,$\sigma^2 \cdot \rho(\boldsymbol{x}) = \rho \cdot \sigma^2(\boldsymbol{x})$. 因此,$\sigma^2 \cdot \rho = \rho \cdot \sigma^2$. 引理得证.

考虑到σ^2变换与σ变换显然满足可交换性质,结合引理1和引理2,容易知σ^2变换与$\overline{G_i}$中的轮变换均可交换,进而σ^2变换与$\overline{G_i}$也可交换. 类似地,σ^2变换与$\overline{H_i}$也可交换.

3.3　动态密码结构的分类

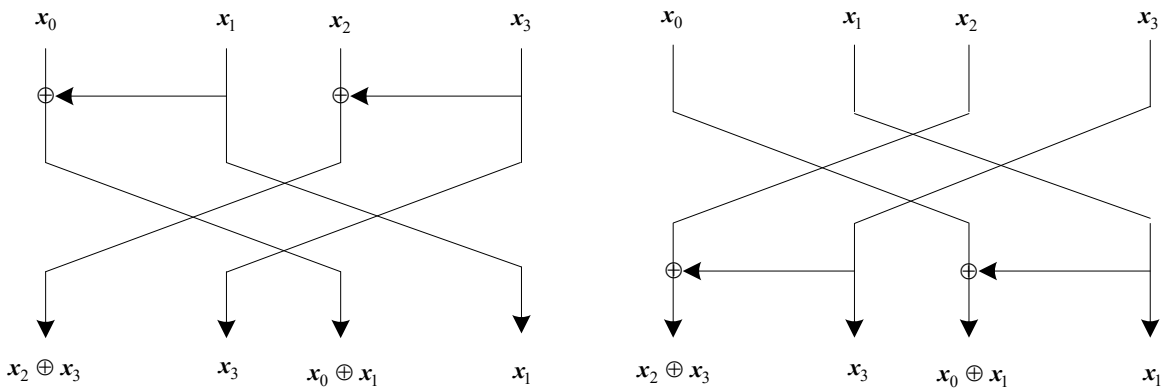
在该小节中,为了研究类CLEFIA动态密码结构C^n和四分组类CLEFIA变换簇L^n的分类,首先给出如下标准单元和标准静态密码结构的定义.

对于动态密码结构C^n,先定义一个标准单元G,它与$\overline{G_i}$唯一区别是将所有循环移位均固定为循环左移,即$G=(\rho\sigma F)\cdot(\sigma F)\cdot(\sigma F)\cdot(\sigma F)$;然后定义一个标准静态密码结构$C^{*n}$,它与$C^n$的等价表示$\overline{C^n}$唯一区别是将所有循环移位均固定为循环左移,也即:

$$C^{*n} = \underbrace{G\cdot G\cdot\cdots\cdot G\cdot G}_{n} \tag{11}$$

对于动态密码结构L^n,类似地,先定义一个标准单元H,它与H_i的等价表示$\overline{H_i}$唯一区别是将所有循环移位均固定为循环左移,即$H=(\sigma F)\cdot(\sigma F)\cdot(\sigma F)\cdot(\sigma F)$;然后定义一个标准静态密码结构$L^{*n}$,它与$L^n$的等价表示$\overline{L^n}$唯一区别是将所有循环移位均固定为循环左移,也即:

$$L^{*n} = \underbrace{H\cdot H\cdot\cdots\cdot H\cdot H}_{n} \tag{12}$$



(*a*) $\sigma^2 \cdot \rho$ (*b*) $\rho \cdot \sigma^2$

图7 ρ变换和σ^2变换的先后复合

在研究动态密码结构的分类时,以类CLEFIA动态密码结构C^n为例,整个研究框架如图8所示. 首先研究动态密码结构中单元G_i的等价表示$\overline{G_i}$与标准静态密码结构中单元G的关系,然后将该关系推广至n个单元,得到$\overline{C^n}$和C^{*n}之间的关系,最后再利用C^n和$\overline{C^n}$的等价关系,即能建立动态密码结构C^n和标准静态密码结构C^{*n}之间的联系.

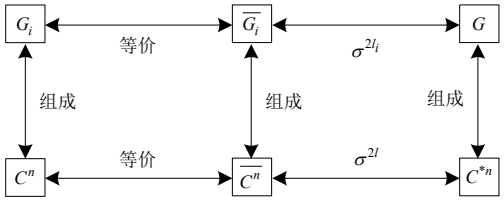


图8 类CLEFIA动态密码结构的等价分类研究框架

下面先通过定理1给出$\overline{G_i}$和G之间的关系.

定理1 对于动态密码结构C^n中的单元$G_i(1 \leqslant i \leqslant n)$,它的等价表示$\overline{G_i}$与标准单元$G$有如下关系:$\overline{G_i} = \sigma^{2l_i}G$,这里$l_i$表示$\overline{G_i}$中$\sigma^{-1}$出现的次数,$0 \leqslant l_i \leqslant 4$.

证明 根据引理1知,σ^2变换和F变换满足可交换的性质,则有

$$F \cdot \sigma^{-1} = F \cdot \sigma^3 = F \cdot \sigma^2 \cdot \sigma = \sigma^2 \cdot F \cdot \sigma \tag{13}$$

故$F \cdot \sigma^{-1} = \sigma^2 \cdot (F \cdot \sigma)$. 考虑到

$$\overline{G_i} = (\rho\sigma^{j_0}F) \cdot (\sigma^{j_1}F) \cdot (\sigma^{j_2}F) \cdot (\sigma^{j_3}F) \tag{14}$$

这里$j_0, j_1, j_2, j_3 \in \{1, -1\}$. 因此

$$\begin{aligned}\overline{G_i} &= (\rho\sigma^{j_0}F) \cdot (\sigma^{j_1}F) \cdot (\sigma^{j_2}F) \cdot (\sigma^{j_3}F) \\ &= \rho\sigma^{j_0} \cdot (F\sigma^{j_1}) \cdot (F\sigma^{j_2}) \cdot (F\sigma^{j_3})F\end{aligned} \tag{15}$$

对于$\sigma^{j_t}(t=0,1,2,3)$,它可以用如下形式表示

$$\sigma^{j_t} = \begin{cases} \sigma, & j_t = 1 \\ \sigma^{-1} = \sigma^3 = \sigma^2 \cdot \sigma, & j_t = -1 \end{cases} \tag{16}$$

式(16)等价于$\sigma^{j_t} = \sigma^{2s_t} \cdot \sigma$,这里$s_t$表示的是$\sigma^{-1}$出现的次数,即

$$s_t = \begin{cases} 0, & j_t = 1 \\ 1, & j_t = -1 \end{cases} \tag{17}$$

对于变换$F \cdot \sigma^{j_t}$,考虑到恒等变换与任何变换均可交换,同时利用引理1,可得:

$$F \cdot \sigma^{j_t} = F \cdot \sigma^{2s_t} \cdot \sigma = \sigma^{2s_t} \cdot (F \cdot \sigma) \tag{18}$$

利用引理1和引理2,可得:

$$\begin{aligned}\overline{G_i} &= \rho\sigma^{j_0} \cdot (F\sigma^{j_1}) \cdot (F\sigma^{j_2}) \cdot (F\sigma^{j_3})F \\ &= (\sigma^{2s_0} \cdot \sigma^{2s_1} \cdot \sigma^{2s_2} \cdot \sigma^{2s_3}) \cdot (\rho\sigma F) \cdot (\sigma F) \cdot (\sigma F) \cdot (\sigma F) \\ &= \sigma^{2(s_0+s_1+s_2+s_3)} \cdot G\end{aligned} \tag{19}$$

令$l_i \triangleq s_0 + s_1 + s_2 + s_3$,则$l_i$表示在单元$\overline{G_i}$中$\sigma^{-1}$出现的次数,$0 \leqslant l_i \leqslant 4$. 故

$$\overline{G_i} = \sigma^{2(s_0+s_1+s_2+s_3)} \cdot G = \sigma^{2l_i} \cdot G \tag{20}$$

定理得证.

对于四分组类CLEFIA变换簇L^n,考虑到$\overline{H_i}$的定义,即在$\overline{H_i}$中4轮循环移位选择要么全为循环左移,要么全为循环右移,则σ^{-1}出现的次数为0或者4,均为偶数. 利用定理1的证明方法,容易得到如下推论.

推论1 对于动态密码结构L^n中的单元$H_i(1 \leqslant i \leqslant n)$,它的等价表示$\overline{H_i}$与标准单元$H$有如下关系:$\overline{H_i} = H$.

进一步,将动态密码结构中单元的等价表示与标准静态密码结构中单元的关系推广至n个单元,并结合动态密码结构的等价表示,建立动态密码结构与标准静态密码结构之间的关系. 下面先通过定理2给出动态密码结构C^n和标准静态密码结构C^{*n}之间的关系.

定理2 动态密码结构C^n置换等价于标准静态密码结构C^{*n},并且有$C^n \sim \overline{C^n} = \sigma^{2l}C^{*n}$,这里$l$表示$\overline{C^n}$中$\sigma^{-1}$出现的次数,$0 \leqslant l \leqslant 4n$.

证明 根据定理1知,$\overline{G_i} = \sigma^{2l_i}G$,这里$l_i$表示$\overline{G_i}$中

σ^{-1}出现的次数,$0\leqslant l_i\leqslant 4$. 由于

$$\begin{aligned}\overline{C^n}&=\overline{G_n}\cdot\overline{G_{n-1}}\cdot\cdots\cdot\overline{G_2}\cdot\overline{G_1}\\&=(\sigma^{2l_n}G)\cdot(\sigma^{2l_{n-1}}G)\cdot\cdots\cdot(\sigma^{2l_2}G)\cdot(\sigma^{2l_1}G)\\&=\sigma^{2(l_n+l_{n-1}+\cdots+l_2+l_1)}\underbrace{G\cdot G\cdot\cdots\cdot G}_{n}\\&=\sigma^{2(l_n+l_{n-1}+\cdots+l_2+l_1)}C^{*n}\end{aligned}\tag{21}$$

令$l\triangleq l_n+l_{n-1}+\cdots+l_2+l_1$,则$l$表示$\overline{C^n}$中$\sigma^{-1}$出现的次数,$0\leqslant l\leqslant 4n$. 则有$\overline{C^n}=\sigma^{2l}C^{*n}$. 又由于$C^n\sim\overline{C^n}$,故$C^n\sim\overline{C^n}=\sigma^{2l}C^{*n}$. 定理得证.

考虑到$\sigma^4=I$,根据定理2知,$\overline{C^n}=\sigma^{2l}C^{*n}$,这里$l$表示$\overline{C^n}$中$\sigma^{-1}$出现的次数,$0\leqslant l\leqslant 4n$. 故,

$$C^n\sim\overline{C^n}=\begin{cases}C^{*n}, & l\bmod 2=0\\ \sigma^2\cdot C^{*n}, & l\bmod 2=1\end{cases}\tag{22}$$

也即,在$4n$轮动态密码结构C^n中,若循环右移σ^{-1}选择的次数为偶数次,则它等价于C^{*n};若循环右移σ^{-1}选择的次数为奇数次,则它等价于$\sigma^2\cdot C^{*n}$. 因此,$4n$轮动态密码结构C^n置换等价于C^{*n}.

对于四分组类CLEFIA变换簇L^n,它的研究框架与动态密码结构C^n相似,如图9所示. 根据推论1,利用定理2的证明思路,容易得到如下推论.

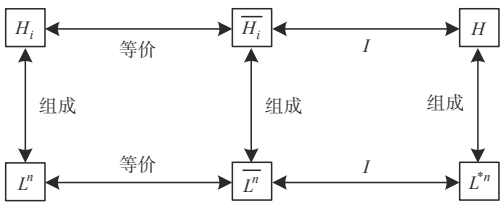


图9　四分组类CLEFIA变换簇的等价分类研究框架

推论2　动态密码结构L^n等价于标准静态密码结构L^{*n},并且有$L^n\sim\overline{L^n}=L^{*n}$.

在文献[11~13]中,他们研究这两类动态密码结构的差分分析和线性分析时,核心思想是通过寻找活跃轮函数的数量来刻画. 而活跃轮函数的定义与非线性组件的具体取值无关,同样是将轮函数视为双射进行研究. 因此,本文对这两类动态密码结构的等价分类,同样能够适用于文献[11~13]. 若利用本文的等价分类结果,能够很大程度上简化文献[11~13]中的证明过程.

从对这两类动态密码结构的安全性分析角度看,本文的等价分类结果对于与轮函数具体细节无关的区分器构造(如不可能差分、零相关线性、中间相遇区分器)或者活跃轮函数的搜索(差分分析、线性分析)有非常重要的指导意义,利用该结果能统一刻画动态密码结构的安全性.

从对这两类动态密码结构的设计角度看,本文的等价分类结果说明若在组件的选取上使得其不完全满足可交换性质,则动态密码结构的安全性刻画难以统一到标准静态密码结构上,此时动态密码结构中不同的结构表现出来的安全强度就会有所区别.

4　动态密码结构的不可能差分和零相关线性区分器构造

利用上节证明的动态密码结构等价分类结果,首先给出动态密码结构和标准静态密码结构之间不可能差分和零相关线性区分器的等价关系,然后通过构造标准静态密码结构的这两种区分器,得到动态密码结构的不可能差分和零相关线性区分器结果.

对于类CLEFIA动态密码结构C^n,根据定理2知,$C^n\sim C^{*n}$或者$C^n\sim\sigma^2\cdot C^{*n}$. 故容易得到如下定理:

定理3　对$4n$轮的动态密码结构C^n和标准静态密码结构C^{*n},若$(a_0,a_1,a_2,a_3)\to(b_0,b_1,b_2,b_3)$是$C^{*n}$的一条$r$轮不可能差分(零相关线性),则$(a_0,a_1,a_2,a_3)\to(b_0,b_1,b_2,b_3)$或者$(a_0,a_1,a_2,a_3)\to(b_2,b_3,b_0,b_1)$是$C^n$一条$r$轮的不可能差分(零相关线性).

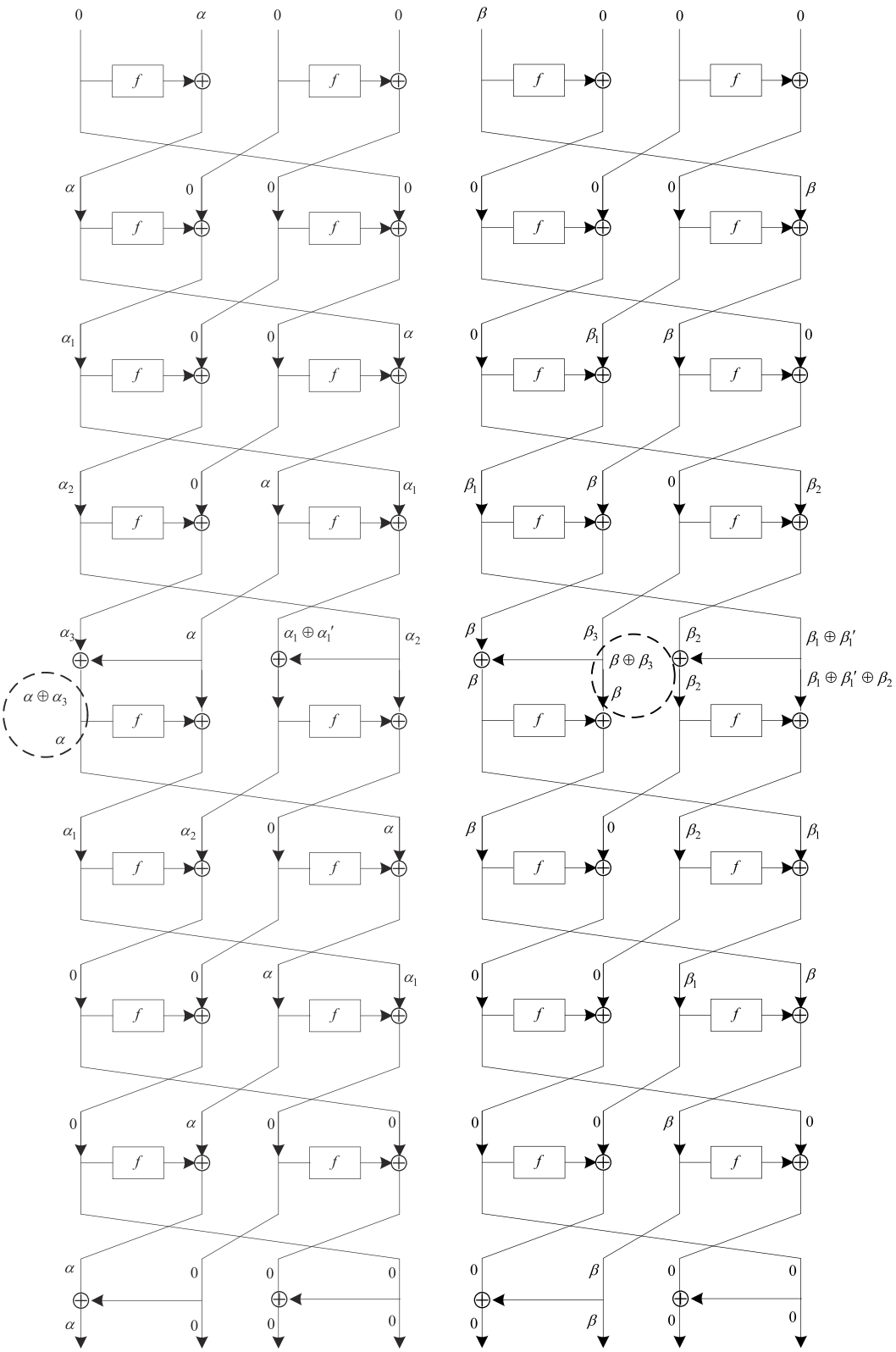
针对标准静态密码结构C^{*n},命题1和命题2分别利用中间相错技术构造了其8轮不可能差分和零相关线性区分器.

命题1　对于标准静态密码结构C^{*n},$(0,\alpha,0,0)\to(\alpha,0,0,0)$是它的一条8轮不可能差分区分器,这里$\alpha$是非零差分.

证明　如图10所示,令$\alpha_i\triangleq\Delta f^i(\alpha)(i=1,2,3)$,其中$\Delta f^i(\alpha)$表示当输入差分为$\alpha$,经过$i$轮$f$函数的差分传播后所有可能的输出差分集合. 下面利用中间相错技术从正向加密和反向解密两个方向来构造矛盾. 从加密方向看,当输入差分$(0,\alpha,0,0)$正向加密传播4轮后,第1个分支的差分为$\alpha\oplus\alpha_3=\alpha\oplus\Delta f^3(\alpha)$;从解密方向看,当输出差分反向解密传播4轮后,第1个分支的差分为α. 若$(0,\alpha,0,0)\to(\alpha,0,0,0)$是一条8轮可能差分,则在中间差分的每一个分支处相等,即需要满足$\alpha\oplus\alpha_3=\alpha\Leftrightarrow\alpha_3=\Delta f^3(\alpha)=0$. 考虑到$f$函数的双射性,$\alpha_3=\Delta f^3(\alpha)=0\Leftrightarrow\alpha=0$,这与$\alpha$非零矛盾. 故$(0,\alpha,0,0)\to(\alpha,0,0,0)$是一条8轮不可能差分.

命题2　对于标准静态密码结构C^{*n},$(\beta,0,0,0)\to(0,\beta,0,0)$是它的一条8轮零相关线性区分器,这里$\beta$是非零掩码.

证明　如图10所示,令$\beta_i\triangleq\Lambda f^{-i}(\beta)(i=1,2,3)$,其中$\Lambda f^{-i}(\beta)$表示当输入掩码为$\beta$,经过$i$轮轮函数的逆$f^1$线性传播后,所有可能的输出掩码集合. 从正向加密和反向解密两个方向利用中间相错技术构造零相关线性区分器. 从加密方向看,当输入掩码$(\beta,0,0,0)$正向加密传播4轮后,第2分支的掩码为$\beta\oplus\beta_3=\beta\oplus\Lambda f^{-3}(\beta)$;从解密方向看,当输出掩码反向解密传播4轮后,第2分支



(*a*) 8轮不可能差分区分器 (*b*) 8轮零相关线性区分器

图10 标准静态密码结构C^{*n}的8轮不可能差分和零相关线性区分器

的掩码为β. 若$(\beta,0,0,0)\to(0,\beta,0,0)$是一条8轮可能线性路径,则在中间掩码的每一个分支处均能相等,即需要满足:$\beta\oplus\beta_3=\beta\Leftrightarrow\beta_3=\Lambda f^{-3}(\beta)=0$. 考虑到$f$函数的双射性,$\beta_3=\Lambda f^{-3}(\beta)=0\Leftrightarrow\beta=0$,这与$\beta$非零矛盾. 因此,$(\beta,0,0,0)\to(0,\beta,0,0)$是一条8轮零相关线性区分器.

利用定理3、命题1和命题2,能够得到如下定理.

定理4　动态密码结构C^n均存在8轮的不可能差分和零相关线性区分器. 进一步,在8轮动态密码结构中,若循环右移选择的次数为偶数,则它均存在形如$(0,\alpha,0,0)\to(\alpha,0,0,0)$的8轮不可能差分区分器和形如$(\beta,0,0,0)\to(0,\beta,0,0)$的8轮零相关线性区分器;若循环右移选择的次数为奇数,则它均存在形如$(0,\alpha,0,0)\to(0,0,\alpha,0)$的8轮不可能差分区分器和形如$(\beta,0,0,0)\to(0,0,0,\beta)$的8轮零相关线性区分器,这里$\alpha$是非零差分,$\beta$是非零掩码.

类似地,根据推论2知,$4n$轮的四分组类CLEFIA变换簇L^n与标准静态密码结构L^{*n}之间关于这两类区分器同样存在一一对应的关系. 根据CLEFIA算法已有的安全性分析结果,文献[17]和文献[18]分别指出CLEFIA具有9轮的不可能差分和零相关线性区分器. 因此,对于$4n$轮的四分组类CLEFIA变换簇L^n,有如下定理.

定理5　动态密码结构L^n均存在9轮的不可能差分和零相关线性区分器. 进一步,它均存在形如$(0,\alpha,0,0)\to(\alpha,0,0,0)$的9轮不可能差分区分器[17]和形如$(\beta,0,0,0)\to(0,0,0,\beta)$的9轮零相关线性区分器[18],这里$\alpha$是非零差分,$\beta$是非零掩码.

5　结束语

针对两类动态密码结构,在轮函数为双射的条件下,通过建立与标准静态密码结构的等价关系,统一刻画了它们概率为1的差分传播和线性传播,进而给出了关于两类动态密码结构统一的不可能差分和零相关线性区分器结果. 该等价刻画方法,为评估动态密码结构抵抗不可能差分和零相关线性分析的能力提供了全新的思路. 与此同时,该方法也为动态密码结构的设计提供了重要的选取准则.

参考文献

[1] DAEMEN J, RIJMEN V. AES proposal: Rijndael[EB/OL]. (1999-09-03) [2022-01-25]. https://www.math.u-bordeaux.fr/~kbelabas/teach/MHT633/Rijndael.pdf.

[2] 国家商用密码管理办公室. 无线局域网产品使用的SMS4密码算法[EB/OL]. (2016-11-18)[2022-01-25]. http://www.oscca.gov.cn/UpFile/2006220264232979 90.Pdf.

[3] SHIRAI T, SHIBUTANI K, AKISHITA T, et al. The 128-bit blockcipher CLEFIA[C]// Proceedings of the 14th International Conference on Fast Software Encryption. Berlin: Springer, 2007: 181-195.

[4] LISKOV M, RIVEST R L, WAGNER D. Tweakable block ciphers[J]. Journal of Cryptology, 2011, 24(3): 588-613.

[5] MOHAMMED MAHMOUD E, ABD EL HAFEZ A, EL-GARF T A, et al. Dynamic AES-128 with key-dependent S-box[J]. International Journal of Engineering Research and Applications, 2013, 3(1): 1662-1670.

[6] SCHNEIER B. Description of a new variable-length key, 64-bit block cipher (Blowfish) [C]//Fast Software Encryption. Berlin: Springer, 1994: 191-204.

[7] ISOBE T. A single-key attack on the full GOST block cipher[J]. Journal of Cryptology, 2013, 26(1):172-189.

[8] 李浪, 李肯立, 贺位位, 等. Magpie: 一种高安全的轻量级分组密码算法[J]. 电子学报, 2017, 45(10): 2521-2527.
LI L, LI K L, HE W W, et al. Magpie: A high-security lightweight block cipher[J]. Acta Electronica Sinica, 2017, 45(10): 2521-2527. (in Chinese)

[9] 王念平, 郭祉成. 动态密码结构抵抗差分密码分析能力评估[J]. 通信学报, 2021, 42(8): 70-79.
WANG N P, GUO Z C. Security evaluation against differential cryptanalysis for dynamic cryptographic structure[J]. Journal on Communications, 2021, 42(8): 70-79. (in Chinese)

[10] 王念平, 殷勍. 类Piccolo结构的差分安全性评估[J]. 通信学报, 2022, 43(2): 55-64.
WANG N P, YIN Q. Differential security evaluation of Piccolo-like structure[J]. Journal on Communications, 2022, 43(2): 55-64. (in Chinese)

[11] 王念平. 四分组类CLEFIA变换簇抵抗差分密码分析的安全性评估[J]. 电子学报, 2017, 45(10): 2528-2532.
WANG N P. Security evaluation against differential cryptanalysis for four-block CLEFIA-like transform cluster[J]. Acta Electronica Sinica, 2017, 45(10): 2528-2532. (in Chinese)

[12] 王念平. 一类分组密码变换簇抵抗线性密码分析的安全性评估[J]. 电子学报, 2020, 48(1): 137-142.
WANG N P. Security evaluation against linear cryptanalysis for a class of block cipher transform cluster[J]. Acta Electronica Sinica, 2020, 48(1): 137-142. (in Chinese)

[13] 杨继林, 王念平. 类CLEFIA动态密码结构抵抗差分密码分析能力评估[J]. 电子学报, 2021, 49(11): 2279-2283.
YANG J L, WANG N P. Security evaluation against differential cryptanalysis for CLEFIA-like dynamic cryptographic structure[J]. Acta Electronica Sinica, 2021, 49

(11): 2279-2283. (in Chinese)
[14] KNUDSEN L. DEAL-A 128-bit Block Cipher[R]. Bergen: University of Bergen, 1998.
[15] BIHAM E, BIRYUKOV A, SHAMIR A. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials[C]//Advances in Cryptology — EUROCRYPT'99. Berlin: Springer, 1999: 12-23.
[16] BOGDANOV A, RIJMEN V. Linear hulls with correlation zero and linear cryptanalysis of block ciphers[J]. Designs, Codes and Cryptography, 2014, 70(3): 369-383.
[17] TSUNOO Y, TSUJIHARA E, SHIGERI M, et al. Impossible differential cryptanalysis of CLEFIA[C]//Fast Software Encryption. Berlin, Heidelberg: Springer, 2008: 398-411.
[18] 崔霆, 金晨辉. 嵌套代替-扩散网络的CLEFIA结构零相关线性逼近的构造[J]. 电子与信息学报, 2012, 34(1): 227-230.
CUI T, JIN C H. Construction of zero-correlation linear hull for CLEFIA-like structure with SPN round functions [J]. Journal of Electronics & Information Technology, 2012, 34(1): 227-230. (in Chinese)

作者简介

沈 璇 男, 1990 年 1 月生, 湖北荆门人, 博士. 现为国防科技大学信息通信学院副教授, 主要研究方向为对称密码的设计与分析.
E-mail: shenxuan_08@163.com

刘国强 男, 1986 年 1 月生, 湖南浏阳人, 博士. 现为国防科技大学理学院副教授, 主要研究方向为对称密码的设计与分析.
E-mail: liuguoqiang87@hotmail.com

孙 兵 男, 1981 年 8 月生, 江苏南通人, 博士. 现为国防科技大学理学院副教授, 主要研究方向为对称密码的设计与分析.
E-mail: happy_come@163.com

何 俊 男, 1979 年 6 月生, 湖北公安人, 博士. 现为国防科技大学信息通信学院教授, 主要研究方向为网络安全.
E-mail: hejun17c@nudt.edu.cn