广义类CLEFIA动态密码结构抵抗差分和线性密码分析的安全性评估

成 磊[1,2,4],沈 璇[3*],任传伦[4]

(1. 电子科技大学计算机科学与工程学院,四川成都 611731;2. 中国电子科技网络信息安全有限公司,四川成都 610041;
3. 国防科技大学信息通信学院,湖北武汉 430010;4. 中国电子科技集团公司第三十六研究所,浙江嘉兴 314033)

摘 要: 基于四分支类CLEFIA动态密码结构,对2m分支类CLEFIA动态密码结构进行分析,证明基于循环变换的类CLEFIA动态密码结构等价于CLEFIA密码结构. 对2m分支类CLEFIA动态密码结构最小差分活动轮函数个数的上界进行研究,证明每轮变换P_i为基于GF(2^s)上{0,1}构成的动态线性变换,2m分支类CLEFIA动态密码结构最小差分活动轮函数上界为$\left\lfloor \frac{2^{2m-1}}{2^{2m}-1} mr \right\rfloor$,其中,$r$为轮数. 另外,可将上述关于差分性质的结果推广得到类CLEFIA动态密码结构线性性质的结果.

关键词: 密码结构;类CLEFIA动态密码结构;差分密码分析;线性密码分析;活动轮函数

基金项目: 国家自然科学基金(No.62227805);国防科技大学科研计划项目(No.ZK21-36)

中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112(2024)08-2571-10

电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20230638

Security Evaluation of Generalized CLEFIA-Like Dynamic Cipher Structures Against Differential and Linear Cryptanalysis

CHENG Lei[1,2,4], SHEN Xuan[3*], REN Chuan-lun[4]

(1. *School of Computer Science and Engineering*, *University of Electronic Science and Technology*, *Chengdu*, *Sichuan* 611731, *China*;
2. *China Electronic Technology Cyber Security Company*, *Chengdu*, *Sichuan* 610041, *China*;
3. *College of Information and Communication*, *National University of Defense Technology*, *Wuhan*, *Hubei* 430010, *China*;
4. *The* 36*th Research Institute of China Electronics Technology Corporation*, *Jiaxing*, *Zhejiang* 314033, *China*)

Abstract: Based on the four-branch CLEFIA-like dynamic cipher structure, this paper analyzes the 2m-branch CLEFIA-like dynamic cipher structure, proving the equivalence between the cyclically permuted transformation-based CLEFIA-like dynamic cipher structure and the CLEFIA cipher structure. Furthermore, the upper bound on the minimum number of differentially active rounds for the 2m-branch CLEFIA-like dynamic cipher structure is investigated. It is demonstrated if each round transformation P_i is the dynamic linear transformation consisting of {0, 1} on GF(2^s), the upper bound on the minimum number of differentially active rounds for the 2m-branch CLEFIA-like dynamic cipher structure is $\left\lfloor \frac{2^{2m-1}}{2^{2m}-1} mr \right\rfloor$, where r denotes the number of rounds. Additionally, the results regarding differential properties can be extended to the linear properties of the CLEFIA-like dynamic cipher structure.

Key words: cryptographic structure; CLEFIA-like dynamic cryptographic structure; differential cryptanalysis; linear cryptanalysis; active round functions

Foundation Item(s): National Natural Science Foundation of China (No.62227805); Scientific Research Plan of National University of Defense Technology (No.ZK21-36)

收稿日期:2023-07-05;修回日期:2023-11-06;责任编辑:梅志强

*通讯作者:沈璇

1 引言

随着信息技术的发展,各类数据迅猛增长,对经济发展和人民生活都产生深刻影响. 数据安全成为事关国家安全与社会发展的重大问题. 使用分组密码是确保数据安全的重要手段之一. 国内外有许多分组密码标准算法,如 AES(Advanced Encryption Standard)[1]、SM4[2]、CLEFIA[3]等. CLEFIA 算法是由 SONY 公司设计,用于保护 SONY 公司的图像和音乐等数字内容,并于 2007 年 FSE 会议上公布. 该算法被广泛应用于各种领域,包括物联网(Internet of Things,IoT)、移动设备和嵌入式系统等,并被列为 ISO/IEC 29192-2 国际标准.

对分组密码算法设计而言,分组密码的安全性分析至关重要. 在当前的密码安全性研究中,差分分析、线性分析及变种是最为常用和重要的分析方法. 差分分析是由 Biham 和 Shamir[4]在 1990 年的 CRYPTO 会议上提出的分析方法,核心是关注明文与密文之间的差异,利用密文差异的不均匀性构建具有高概率的差分区分器. 线性分析则是由日本学者 Matsui[5]在 1993 年的 EUROCRYPT 会议上提出的分析方法,主要考虑明文与密文之间的线性关系,并基于线性谱的不均匀特性构建具有较大线性偏差的区分器. 在评估分组密码对差分分析和线性分析的抵抗能力时,活动轮函数或活动 S 盒的个数成为重要安全性评估指标,对算法起着重要作用. 针对具体算法,最小差分活动 S 盒数目往往采用计算机搜索方法,常用的有 Matsui 分支定界算法[5]、基于混合整数线性规划(Mixed-Integer Linear Programming,MILP)[6]和基于布尔可满足性(boolean SATisfiability problem,SAT)方法[7]. 分支定界方法主要是将差分活动 S 盒搜索转化为搜索树,通过回溯和剪枝逐步缩小搜索空间. MILP 方法和 SAT 方法都是将最小差分活动 S 盒搜索问题转化为 MILP 问题和 SAT 问题,利用求解器求解. Mouha 等人[6]提出针对异或操作和线性变换的 MILP 模型,将面向字节分组密码算法的最小差分/线性活动 S 盒个数问题转化为 MILP 问题,并利用通用求解器进行求解. Sun 等人[8]进一步将 MILP 方法应用到面向比特的密码算法,基于 MILP 方法求解最小活动 S 盒个数和最优(相关密钥)差分/线性特征搜索. 随着密码分析自动化搜索研究的不断开展,MILP 方法已经被广泛应用于各种密码分析,包括差分分析[8,9]、不可能差分分析[10]、积分分析[11,12]和立方分析[13~15]等. Li 等人[16]提出超级球的方法用于产生 MILP 模型中的不等式,基于未确定系数方法生成不同类型的不等式描述,从而能够对不同类型不等式描述进行比较. Bellini 等人[17]基于 ChaCha 算法提出新的 MILP 模型,能更好地覆盖搜索空间,找到 1 条从第 3~7 轮线性相关性更高的线性特征,并给出 7 轮 ChaCha 算法的差分-线性攻击.

美国国家标准与技术研究所(National Institute of Standards and Technology,NIST)于 2015 年启动轻量级加密标准化过程,要求加密方案在受限环境下支持对关联数据认证加密(Authenticated Encryption with Associated Data,AEAD)以及可选哈希功能. 经过 3 轮筛选,最后于 2021 年 3 月公布 10 个候选算法,包括支持 AEAD 功能的 5 个算法:基于置换设计的算法 Elephant[18]和 ISAP[19]、基于分组密码算法 GIFT-COFB[20]和 TinyJAMBU[21]、基于流密码算法 Grain-128AEAD[22]. 支持 AEAD 和哈希功能的 5 个算法:基于置换设计的算法 ASCON[23]、PHOTON-Beetle[24]、SPARKLE[25]和 Xoodyak[26],基于可调分组密码算法 Romulus[27]. NIST 在 2023 年 2 月 7 日宣布将 ASCON 家族系列算法进行标准化[28]. ASCON[29]家族支持 AEAD 和哈希功能及可扩展函数(XOFs)等不同功能,满足程序广泛应用的要求. ASCON 系列算法是基于 320 bit 的置换设计,不同变种选择不同常数和轮数. ASCON 算法凭借优秀的软硬件实现能力和高安全冗余度及灵活调整等特点,最终在评选中胜出. 另外,ASCON 算法是在 CAESAR 竞赛中资源受限环境下胜出.

为了提高加密算法对分析攻击的抵抗能力,学者们在密码设计中引入动态思想,提出动态密码结构的概念. 这种方法通过利用算法的中间状态或参数来控制密码算法的各组件,如 S 盒、线性变换等,实现密码结构的动态变化. 动态密码结构分为 3 种类型:第 1 种是通过中间状态来控制算法组件,如 CAST-256[30]和 RC6 算法[31];第 2 种是可调分组密码,通过与中间状态进行异或操作的调节来实现[32,33]. 在轻量级密码标准化中,许多方案都采用可调分组密码的方法,例如 GIFT-COFB[34]和 Spook[35]等;最后 1 种是通过独立参数来选择组件,不同的参数选择会导致使用不同备选组件[36~38].

2017 年,王念平等人[39]提出四分组类 CLEFIA 变换簇,每 4 轮为 1 个单元,每个单元中的块移位变换相同,要么循环左移要么循环右移,并对变换簇中密码结构抗差分的分析能力进行评估. 2020 年王念平[40]对四分组类 CLEFIA 变换簇线性密码分析的安全性进行评估,提出需要进一步研究的 2 个问题. 2021 年,王念平等人[41]借鉴“四分组类 CLEFIA 变换簇”的设计思想,设计提出“类 CLEFIA 动态密码结构”,每 6 轮的最后 1 轮中扩散层从多个 $GF(2)^4$ 上的线性变换选取,其余 5 轮都是 CLEFIA 结构,也就是每 6 轮中最后 1 轮进行动态变化. 同时,对该动态密码结构差分性质进行分析,给出 r 轮差分活动轮函数个数下界为 r 或者 $r-1$. 杨继林等人[42]在 2021 年基于动态思想提出“类 CLEFIA 动态密码结构”,每轮块移位都在循环左移和循环右移中进行

选择. 同时,每4轮变换后添加1个反向的异或变换,称第4轮为变形密码结构. 通过对动态密码结构差分性质分析,证明r轮差分特征至少有$r-1$个活动轮函数,提出该结构关于线性活动轮函数和其他线性变换结果的问题,如表1所示. 此外,沈璇等人[43]在2024年还给出了该类动态密码结构不可能差分和零相关线性的对偶关系.

除了研究不同密码动态结构的最小活动轮函数下界,王念平等人[44]2021年通过对类MARS密码结构的研究,证明无论怎样设计线性变换,都存在1条活动轮函数个数不超过$\lfloor 8r/15 \rfloor$的线性逼近,即最小线性活动轮函数上界不超过$\lfloor 8r/15 \rfloor$,其中,r为轮数. 从而对线性变换设计给出指导,避免设计的线性变换过于复杂.

表1　类CLEFIA动态结构的安全性评估

分析方法	密码结构	活动轮函数个数分析	来源文献
差分分析	四分组类CLEFIA变换簇	$\geqslant r-\lfloor (r \bmod 6)/6 \rfloor$	文献[39]
	基于CLEFIA动态密码结构	$\geqslant \begin{cases} r, & r=6t\,(t\geqslant 1) \text{ or } r=6t+1\,(t\geqslant 3) \\ r-1, & \text{other} \end{cases}$	文献[42]
	类CLEFIA动态密码结构	$\geqslant r-1$	文献[41]
	四分组类CLEFIA变换簇 基于CLEFIA动态密码结构 类CLEFIA动态密码结构	$\leqslant \left\lfloor \frac{16}{15}r \right\rfloor = \left\lfloor r+\frac{1}{15}r \right\rfloor = r+\left\lfloor \frac{1}{15}r \right\rfloor$	本文
线性分析	四分组类CLEFIA变换簇	$\geqslant r-\lfloor (r \bmod 6)/6 \rfloor$	文献[40]
	四分组类CLEFIA变换簇 基于CLEFIA动态密码结构 类CLEFIA动态密码结构	$\leqslant \left\lfloor \frac{16}{15}r \right\rfloor = \left\lfloor r+\frac{1}{15}r \right\rfloor = r+\left\lfloor \frac{1}{15}r \right\rfloor$	本文

下面详细给出上述文献中提出的问题,本文的部分结果对这些问题进行回答.

问题1[40]: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他2个不同的块移位变换时,类似定理2的结论未必成立,那这2个不同的块移位变换满足什么条件时,才有类似定理2的结论成立?

问题2[40]:类似于四分组类CLEFIA变换簇,可以定义$m(m>4)$分组类CLEFIA变换簇,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?这里的m分组,是指将输入分成m个分块的情形.

问题3[41]:类CLEFIA动态密码结构的线性密码分析结果如何? 将其中的循环移位变换替换成其他线性变换时,是否有类似结论成立?

2　预备知识

2.1　有关定义

不妨设GF(2)为二元域,GF(2^n)和GF(2^s)为GF(2)上的n维和s维线性空间. 设输入差分$\boldsymbol{\delta}=(\delta_1,\delta_2,\cdots,\delta_n)\in \mathrm{GF}(2^n)$和输出差分$\boldsymbol{\Delta}=(\Delta_1,\Delta_2,\cdots,\Delta_s)\in \mathrm{GF}(2^s)$,那么输入差分$\boldsymbol{\delta}$和输出差分$\boldsymbol{\Delta}$的差分概率为

$$p(\boldsymbol{\delta}\xrightarrow{F}\boldsymbol{\Delta})\triangleq \frac{\#\{\boldsymbol{x}\in \mathrm{GF}(2^n)\mid F(\boldsymbol{x})\oplus F(\boldsymbol{x}\oplus\boldsymbol{\delta})=\boldsymbol{\Delta}\}}{2^n} \tag{1}$$

其中,$\#\{\cdot\}$表示集合的元素数目. 本文中轮函数F是双射,因此有$n=s$,即F是GF(2^s)上的双射函数. 进一步给出差分活动轮函数的定义:

定义1[4]　设$\boldsymbol{\delta}\to\boldsymbol{\Delta}$是轮函数$F$的差分特征,即$p(\boldsymbol{\delta}\xrightarrow{F}\boldsymbol{\Delta})>0$,若$\boldsymbol{\delta}\neq 0$,则称该轮函数$F$为差分活动轮函数.

设$\boldsymbol{u}=(u_1,u_2,\cdots,u_n)$,$\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in \mathrm{GF}(2^n)$,则

$$\boldsymbol{u}\cdot\boldsymbol{x}^{\mathrm{T}}\triangleq u_1x_1\oplus u_2x_2\oplus\cdots\oplus u_nx_n \tag{2}$$

式(2)称为$\boldsymbol{u}$和$\boldsymbol{x}$的内积. F是1个GF(2^n)→GF(2^s)的函数,那么

$$c(\boldsymbol{u}\xrightarrow{F}\boldsymbol{v})\triangleq \frac{1}{2^n}\sum_{\boldsymbol{x}\in \mathrm{GF}(2^n)}(-1)^{\boldsymbol{u}\cdot\boldsymbol{x}^{\mathrm{T}}\oplus\boldsymbol{v}\cdot\boldsymbol{x}_F^{\mathrm{T}}} \tag{3}$$

是以$\boldsymbol{u}$为输入掩码和$\boldsymbol{v}$为输出掩码的线性相关度,其中$\boldsymbol{u}\in \mathrm{GF}(2^n)$,$\boldsymbol{v}\in \mathrm{GF}(2^s)$. 类似地,给出线性活动轮函数的定义.

定义2[5]　设$\boldsymbol{u}\to\boldsymbol{v}$是轮函数$F$的1个线性特征,即$c(\boldsymbol{u}\xrightarrow{F}\boldsymbol{v})\neq 0$,若$\boldsymbol{v}\neq 0$,则称该轮函数$F$为线性活动轮函数.

2.2　广义类CLEFIA动态密码结构

Zheng等人[36]设计提出的Type-II广义Feistel结构被广泛应用于密码算法的设计中. 基于该结构,Shirai等人[37]设计CLEFIA分组密码算法,本文将Type-II型广义Feistel结构称为CLEFIA结构. 下面给出广义$2m$分支CLEFIA密码结构和动态密码结构的相关概念.

定义3　$2m$分支CLEFIA密码结构. 设$(x_0,x_1,\cdots,x_{2m-1})\in(\mathrm{GF}(2^s))^{2m}$和$(z_0,z_1,\cdots,z_{2m-1})\in(\mathrm{GF}(2^s))^{2m}$表示轮加密的输入和输出,$(y_0,y_1,\cdots,y_{2m-1})\in(\mathrm{GF}(2^s))^{2m}$为中间状态,如图1所示,$2m$分支CLEFIA密码结构满足式(4):

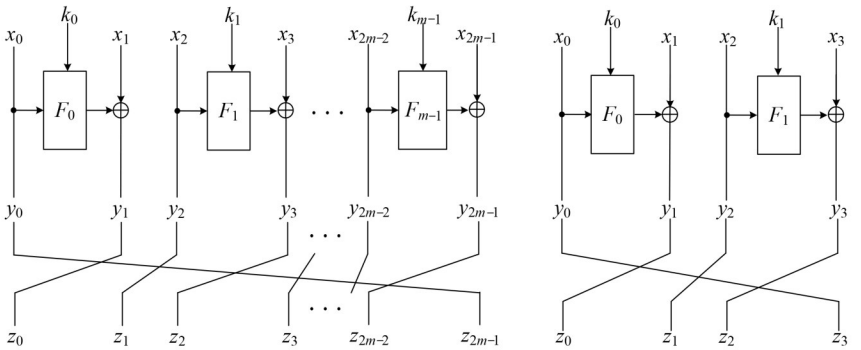

图1 2m分支CLEFIA密码结构和四分支CLEFIA密码结构

$$\begin{cases} y_0=x_0 \\ y_1=x_1\oplus F_0\cdot(x_0\oplus k_0) \\ \quad\vdots \\ y_{2m-2}=x_{2m-2} \\ y_{2m-1}=x_{2m-1}\oplus F_{m-1}\cdot(x_{2m-2}\oplus k_{m-1})\cdot(z_0,z_1,\cdots,z_{2m-1}) \\ \quad\quad =L_{2m}^{1}\cdot(y_0,y_1,\cdots,y_{2m-1}) \\ \quad\quad =(y_1,y_2,\cdots,y_{2m-1},y_0) \end{cases} \tag{4}$$

其中，L_{2m}^{1}表示2m分支循环左移1个分支，轮函数$F_i(0\leqslant i\leqslant m-1)$一般是非线性轮函数，如图1所示．实际算法中轮函数往往采用SP结构或ARX结构实现．当m=2，则称为四分支CLEFIA密码结构，具体表示为$(x_0,x_1,x_2,x_3)\in(\mathrm{GF}(2^s))^4$和$(z_0,z_1,z_2,z_3)\in(\mathrm{GF}(2^s))^4$表示加密的输入和输出，$(y_0,y_1,y_2,y_3)\in(\mathrm{GF}(2^s))^4$为中间状态，有

$$\begin{cases} z_3=y_0=x_0 \\ z_0=y_1=x_1\oplus F_0\cdot(x_0\oplus k_0) \\ z_1=y_2=x_2 \\ z_2=y_3=x_3\oplus F_1\cdot(x_2\oplus k_1) \end{cases} \tag{5}$$

下面给出2m分支类CLEFIA动态密码结构的定义，2m分支类CLEFIA动态密码结构与CLEFIA密码结构的区别主要是中间状态$(y_0,y_1,\cdots,y_{2m-1})$到输出状态$(z_0,z_1,\cdots,z_{2m-1})$的线性变换$P_i$，后者每轮都是循环左移1个分支变化$L_{2m}^{1}$，前者$P_i$是基于$\mathrm{GF}(2^s)$上的线性变换，且每轮可动态变化，其中，$1\leqslant i\leqslant r$.

定义4 2m分支类CLEFIA动态密码结构．设$(x_0,x_1,\cdots,x_{2m-1})\in(\mathrm{GF}(2^s))^{2m}$和$(z_0,z_1,\cdots,z_{2m-1})\in(\mathrm{GF}(2^s))^{2m}$表示轮加密的输入和输出，$(y_0,y_1,\cdots,y_{2m-1})\in(\mathrm{GF}(2^s))^{2m}$为中间状态，如图2所示，2$m$分支类CLEFIA动态密码结构满足式(6)：

$$\begin{cases} y_0=x_0 \\ y_1=x_1\oplus F_0\cdot(x_0\oplus k_0) \\ \quad\vdots \\ y_{2m-2}=x_{2m-2} \\ y_{2m-1}=x_{2m-1}\oplus F_{m-1}\cdot(x_{2m-2}\oplus k_{m-1}) \\ (z_0,z_1,\cdots,z_{2m-1})=P_i\cdot(y_0,y_1,\cdots,y_{2m-1}) \end{cases} \tag{6}$$

其中，P_i为基于$\mathrm{GF}(2^s)$上的线性变换，并且每轮动态变化．P_i均为循环变换，用L_{2m}^{a}表示左循环移位a块，有

$$\begin{aligned} &L_{2m}^{a}\cdot(y_0,y_1,\cdots,y_{2m-1}) \\ &\quad=(y_0,y_1,\cdots,y_{2m-1})<<<a \\ &\quad=(y_a,y_{(a+1)\bmod 2m},y_{(a+2)\bmod 2m},\cdots,y_{(a-1)\bmod 2m}) \end{aligned} \tag{7}$$

并且$1\leqslant a\leqslant 2m-1$，$a$不能为偶数．若$a$为偶数，前后2轮的加密并没有起到块与块之间的扩散作用，所以这里只考虑a为奇数的情况．将上述结构称为基于循环变换类CLEFIA动态密码结构．当m=2时，则称四分支类CLEFIA动态密码结构，如图2所示，$(x_0,x_1,x_2,x_3)\in(\mathrm{GF}(2^s))^4$和$(z_0,z_1,z_2,z_3)\in(\mathrm{GF}(2^s))^4$为轮加密的输入和输出，$(y_0,y_1,y_2,y_3)\in(\mathrm{GF}(2^s))^4$为中间状态：

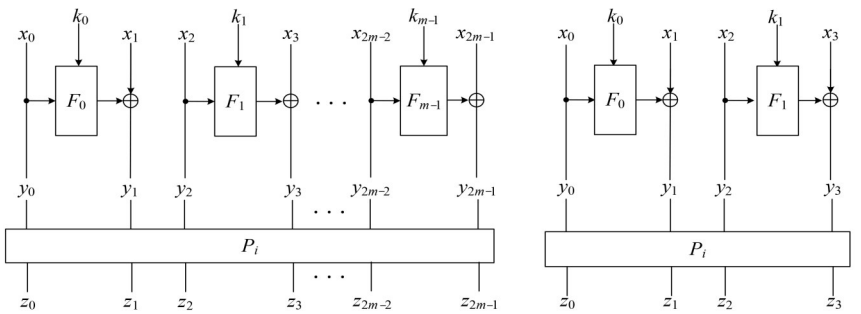

图2 2m分支CLEFIA动态密码结构和四分支类CLEFIA动态密码结构

$$\begin{cases} y_0=x_0 \\ y_1=x_1\oplus F_0\cdot(x_0\oplus k_0) \\ y_2=x_2 \\ y_3=x_3\oplus F_1\cdot(x_2\oplus k_1) \\ (z_0,z_1,z_2,z_3)=P_i\cdot(y_0,y_1,y_2,y_3) \end{cases} \tag{8}$$

3　广义类CLEFIA动态密码结构

定理1　广义$2m$分支基于循环变换类CLEFIA动态密码结构差分性质等价于$2m$分支CLEFIA结构.

证明　分析密码结构的差分和线性性质时,可忽略轮密钥的作用,以差分性质为例进行分析,设$2m$分支的输入和输出差分分别为$(\Delta x_0,\Delta x_1,\cdots,\Delta x_{2m-1})\in(\mathrm{GF}(2^s))^{2m}$和$(\Delta z_0,\Delta z_1,\cdots,\Delta z_{2m-1})\in((\mathrm{GF}(2^s))^{2m}$,轮函数中的动态块置换为$L_{2m}^{a_i}$,其中$1\leqslant i\leqslant r$. 则有$(\Delta y_0,\Delta y_1,\cdots,\Delta y_{2m-1})=R\cdot(\Delta x_0,\Delta x_1,\cdots,\Delta x_{2m-1})$.

$$\begin{cases} \Delta y_0=\Delta x_0 \\ \Delta y_1=\Delta x_1\oplus F\cdot(\Delta x_0) \\ \quad\vdots \\ \Delta y_{2m-2}=\Delta x_{2m-2} \\ \Delta y_{2m-1}=\Delta x_{2m-1}\oplus F\cdot(\Delta x_{2m-2}) \end{cases} \tag{9}$$

和

$$\begin{aligned}&(\Delta z_0,\Delta z_1,\cdots,\Delta z_{2m-1})\\&=L_{2m}^{a_i}\cdot(\Delta y_0,\Delta y_1,\cdots,\Delta y_{2m-1})\\&=(\Delta y_{a_i},\Delta y_{a_i+1},\cdots,\Delta y_{a_i-2},\Delta y_{a_i-1})\end{aligned} \tag{10}$$

其中,$a_i(1\leqslant i\leqslant r)$均为奇数. 注意到变换$R$和$L_{2m}^{2l}$满足交换律,$l$为正整数,有

$$\begin{aligned}&L_{2m}^{2l}R\cdot(\Delta x_0,\Delta x_1,\cdots,\Delta x_{2m-1})\\&=RL_{2m}^{2l}\cdot(\Delta x_0,\Delta x_1,\cdots,\Delta x_{2m-1})\end{aligned} \tag{11}$$

同时,由于左循环变换也满足交换律,有$L_{2m}^{a}L_{2m}^{b}=L_{2m}^{a+b}=L_{2m}^{b}L_{2m}^{a}$. 根据上述性质可证明$2m$分支类CLEFIA动态密码结构的差分性质等价于$2m$分支CLEFIA密码结构,如图3所示,有

$$\begin{aligned}&L_{2m}^{a_r}R\cdots L_{2m}^{a_2}RL_{2m}^{a_1}R\cdot(\Delta x_0,\Delta x_1,\cdots,\Delta x_{2m-1})\\&=L_{2m}^{a_r-1}L_{2m}^{1}R\cdots L_{2m}^{a_2-1}L_{2m}^{1}RL_{2m}^{a_1-1}L_{2m}^{1}R\cdot(\Delta x_0,\Delta x_1,\cdots,\Delta x_{2m-1})\\&=L_{2m}^{a_r-1}\cdots L_{2m}^{a_2-1}L_{2m}^{a_1-1}L_{2m}^{1}RL_{2m}^{1}R\cdots L_{2m}^{1}R\cdot(\Delta x_0,\Delta x_1,\cdots,\Delta x_{2m-1})\\&=L_{2m}^{\sum_{i=1}^{r}a_i-r}(L_{2m}^{1}R)^r\cdot(\Delta x_0,\Delta x_1,\cdots,\Delta x_{2m-1})\end{aligned} \tag{12}$$

其中,$L_{2m}^{a_r}R\cdots L_{2m}^{a_2}RL_{2m}^{a_1}R$表示$r$轮$2m$分支类CLEFIA动态密码结构,$a_i$为第$i$轮的循环参数,$(L_{2m}^{1}R)^r$表示$r$轮$2m$分支CLEFIA密码结构. 由于轮数$r$的任意性,式(12)证明$2m$分支类CLEFIA动态密码结构与$2m$分支CLEFIA密码结构具有相同的差分性质. 通过分析$2m$分支CLEFIA密码结构的差分性质推导基于循环移位分支类CLEFIA动态密码结构的性质.

定理1回答文献[40]中问题1. 一方面解释文献中

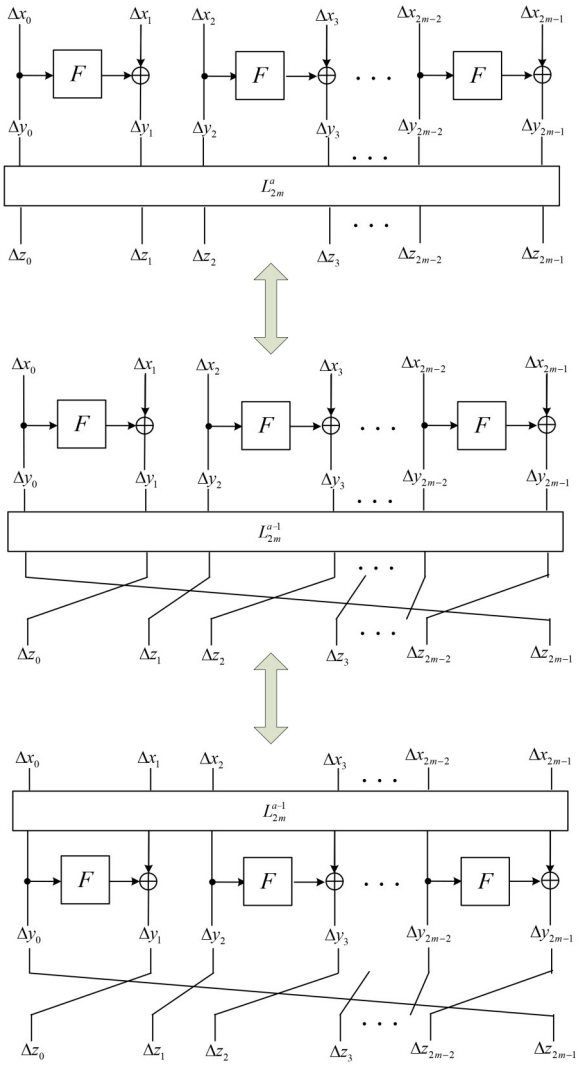

图3　$2m$分组类CLEFIA动态密码结构的差分性质等价示意图

四分支类CLEFIA结构中循环左移变换和循环右移变换有相同个数的差分活动轮函数,四分支循环右移1就是循环左移3,动态结构等价于四分支CLEFIA结构,所以具有相同数目的差分活跃轮数. 另一方面,结合定理1的证明过程,可知若2个块线性变换P_0和P_1,满足以下2个条件:

$$\begin{cases} P_1=P_0Q^{(0,1)}=Q^{(0,1)}P_0 \\ Q^{(0,1)}R=RQ^{(0,1)} \end{cases} \tag{13}$$

那么P_0和P_1也有类似于文献[40]中定理2的结论,也就给出满足问题1中函数的充分条件.

文献[40]的问题2是对于一般m分支类CLEFIA变换簇是否有类似结论,从上述定理可知,对$2m$分支类CLEFIA动态密码结构同样存在相似结论. 这是由于左循环移动变换参数为奇数时,动态密码结构差分性质等价于$2m$分支CLEFIA密码结构,所以$2m$分支类CLEFIA动态密码结构具有相同的差分性质,

如最小活动轮函数,不可能差分等. 另外根据问题1的回答,可进一步分析不同函数之间需要满足的条件.

备注1 四分支CLEFIA密码结构的差分传播与线性传播相似,如图4所示. 若结构的输入差分为$(\Delta x_0,\Delta x_1,\Delta x_2,\Delta x_3)$,单轮加密的对应输出差分为$(\Delta x_1\oplus\Delta y_0,\Delta x_2,\Delta x_3\oplus\Delta y_2,\Delta x_0)$. 而结构的输入掩码为$(\Gamma x_0,\Gamma x_1,\Gamma x_2,\Gamma x_3)$,单轮加密的输出掩码为$(\Gamma x_1,\Gamma x_2\oplus\Gamma y_3,\Gamma x_3,\Gamma x_0\oplus\Gamma y_1)$. 因此,关于线性传播也具有相似的结果.

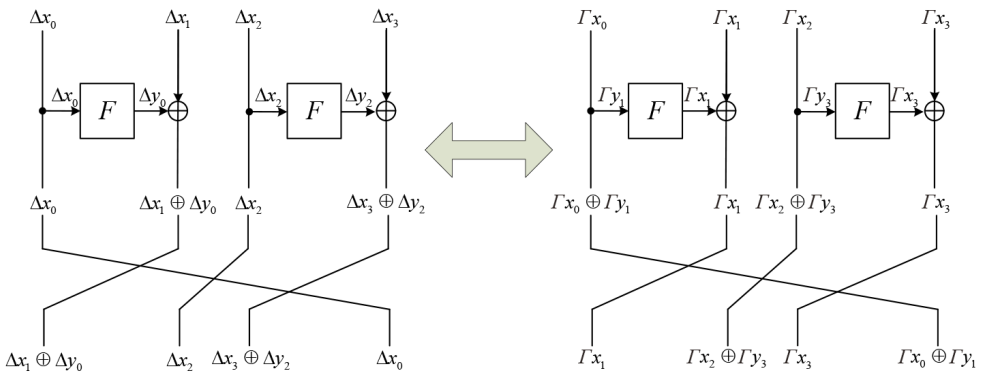

图4 四分支CLEFIA结构的差分和线性性质等价示意图

定理2 广义$2m$分支基于循环变换类CLEFIA动态密码结构线性性质等价于$2m$分支CLEFIA结构.

4 广义类CLEFIA动态密码的安全性评估

不同文献分别给出四分支类CLEFIA动态密码结构中不同的动态变换,如"类CLEFIA动态密码结构"[42]中每6轮中最后1轮进行动态变换,文献[41]中每4轮进行相同循环变换,并在最后1轮加反馈异或等,本节对上述动态密码结构的最小差分活动轮函数进行研究. 重点分析动态密码结构中最小差分活动轮函数个数的上界,并证明上述结构均满足该上界. 借鉴王念平等人[44]的证明思路,构造某条差分特征,因最小差分活动轮函数个数一定不大于任意差分特征的活动轮函数,故某条差分特征活动轮函数个数就是最小差分活动轮函数上界. 为方便描述,针对$2m$分支CLEFIA密码结构进行证明,将证明过程的关键点推广到基于$(\mathrm{GF}(2^s)$上$\{0,1\}$构成的线性变换,使基于$(\mathrm{GF}(2^s)$上$\{0,1\}$的线性动态变化的CLEFIA密码结构同样具有如下性质.

定理3 $2m$分支CLEFIA密码结构的最小差分活动轮函数个数$\leqslant\left\lfloor\frac{2^{2m-1}}{2^{2m}-1}mr\right\rfloor$,其中,$2m$为广义类CLEFIA的分支个数,$r$表示轮数.

证明

首先构造1个特殊的非零差分集合,有如下条件:

$$\begin{aligned}\boldsymbol{\Delta}_{2m}=(0,\boldsymbol{\delta})^{2m}=\{&(0,0,\cdots,0)\neq(\Delta x_0,\Delta x_1,\cdots,\Delta x_{2m-1})\\&\in(\mathrm{GF}(2^s))^{2m}|\Delta x_i\in\{0,\boldsymbol{\delta}\},0\leqslant i\leqslant 2m-1\}\end{aligned}\tag{14}$$

并且$\left|\boldsymbol{\Delta}_{2m}\right|=2^{2m}-1$,其中,$0\neq\boldsymbol{\delta}\in\mathrm{GF}(2^s)$为分支上某个固定差分. 进一步分析结构差分性质,一般轮函数F满足$p(\boldsymbol{\delta}\xrightarrow{F}\boldsymbol{\beta})>0$,其中,$\boldsymbol{\delta}$、$\boldsymbol{\beta}$均为非零差分. 特别地,选择$\boldsymbol{\delta}=\boldsymbol{\beta}$进行差分传播,即有

$$\begin{cases}p(0\xrightarrow{F}0)>0\\p(\boldsymbol{\delta}\xrightarrow{F}\boldsymbol{\delta})>0\end{cases}\tag{15}$$

因此,若每个分支的输入差分均为$\{0,\boldsymbol{\delta}\}$,那么轮函数$F$的差分规则可视为恒等变换,如图5所示. 若输入差分$(\Delta x_0,\Delta x_1,\cdots,\Delta x_{2m-1})$遍历非零差分集合$\boldsymbol{\Delta}_{2m}$,那么由于轮函数$F$为恒等变换,因此,中间差分$(\Delta y_0,\Delta y_1,\cdots,\Delta y_{2m-1})$相应也遍历非零差分集合$\boldsymbol{\Delta}_{2m}$,并且不同的输入差分$(\Delta x_0,\Delta x_1,\cdots,\Delta x_{2m-1})$对应的$(\Delta y_0,\Delta y_1,\cdots,\Delta y_{2m-1})$也不同. $2m$分支CLEFIA结构的左循环变换为L^1_{2m},那么输出差分$(\Delta z_0,\Delta z_1,\cdots,\Delta z_{2m-1})$同样遍历集合$\boldsymbol{\Delta}_{2m}$,同时$(\Delta x_0,\Delta x_1,\cdots,\Delta x_{2m-1})$不同对应的$(\Delta z_0,\Delta z_1,\cdots,\Delta z_{2m-1})$也不同. 由于每轮都具有上述性质,因此,$2m$分支类CLEFIA动态密码结构均满足上述性质.

下面按照上述差分传播规则,由差分集合$\boldsymbol{\Delta}_{2m}$构成的$2^{2m}-1$条差分特征,由于每轮输入差分都遍历集合$\boldsymbol{\Delta}_{2m}$,因此,每轮共$2^{2m-1}m$个差分活动轮函数,那么$2^{2m}-1$条r轮差分特征共有$2^{2m-1}mr$个差分活动轮函数,所以存在某条r轮差分特征的活动轮函数个数$\leqslant\left\lfloor\frac{2^{2m-1}}{2^{2m}-1}mr\right\rfloor$,那么相应的最小差分活动轮函数个数$\leqslant\left\lfloor\frac{2^{2m-1}}{2^{2m}-1}mr\right\rfloor$.

备注2 虽然上面是关于$2m$分支CLEFIA密码结构结果,但是对该证明过程进行分析,关键点在于输入

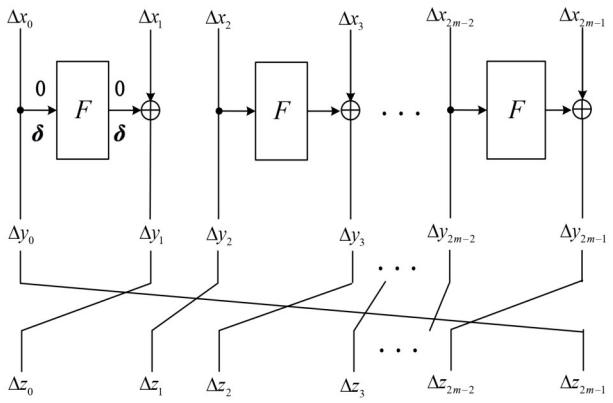

图5　2m分组CLEFIA结构

差分集合$(\Delta x_0, \Delta x_1, \cdots, \Delta x_{2m-1})$遍历$\boldsymbol{\Delta}_{2m}$时，中间差分$(\Delta y_0, \Delta y_1, \cdots, \Delta y_{2m-1})$和输出差分$(\Delta z_0, \Delta z_1, \cdots, \Delta z_{2m-1})$也相应遍历$\boldsymbol{\Delta}_{2m}$，并满足不同$(\Delta x_0, \Delta x_1, \cdots, \Delta x_{2m-1})$相应的中间差分和输出差分也不相同. 注意到将循环变化L_{2m}^i推广为基于GF(2^s)上$\{0,1\}$的线性变换，同样满足若中间差分$(\Delta y_0, \Delta y_1, \cdots, \Delta y_{2m-1})$遍历$\boldsymbol{\Delta}_{2m}$，那么输出差分$(\Delta z_0, \Delta z_1, \cdots, \Delta z_{2m-1})$也遍历$\boldsymbol{\Delta}_{2m}$，因此定理3的结果对基于GF($2^s$)上$\{0,1\}$的线性变换CLEFIA动态密码结构仍然成立，即有如下定理.

定理4　2m分支类CLEFIA动态密码结构的最小差分活动轮函数个数$\leqslant \left\lfloor \frac{2^{2m-1}}{2^{2m}-1} mr \right\rfloor$，其中，2$m$为广义类CLEFIA的分支个数，$r$表示轮数，$P_i$为基于GF($2^s$)上$\{0,1\}$构成的动态线性变换.

备注3　上述证明结果能够广泛推广，适用于每轮P_i的动态变化. 但分析具体结构，可得出精确结果，如考虑m=2的情况，那么四分支CLEFIA密码结构最小差分活动轮函数个数$\leqslant \left\lfloor \frac{16}{15} r \right\rfloor = \left\lfloor r + \frac{1}{15} r \right\rfloor = r + \left\lfloor \frac{1}{15} r \right\rfloor$，实际中可对$\boldsymbol{\Delta}_{2m}$集合中的15个不同输入差分进行遍历，并统计相应的差分活动轮函数个数. 注意到四分支CLEFIA结构输入差分左循环2个分支，结果一致，可进一步减少$\boldsymbol{\Delta}_{2m}$遍历的输入差分数目. 由定理1，可将结果推广到基于循环变化的CLEFIA动态密码结构.

备注4　定理3中关于广义CLEFIA动态密码结构的结果用于指导算法设计，尤其是动态变化的选择. 以四分支类CLEFIA动态密码结构为例，由定理3可知，即使每轮都为基于GF(2^s)上$\{0,1\}$构成的动态线性变换，对应结构的最小差分活动轮函数上界为$r + \left\lfloor \frac{1}{15} r \right\rfloor$，其中，$r$为轮数，表1给出20轮以内的上界结果. 针对具体的CLEFIA密码结构，表2中也给出20轮以内的最小差分活动轮函数的数目. 比较这2行表明循环移位变化改为基于GF(2^s)上$\{0,1\}$构成的动态线性变换，最小差分活动轮函数可能增加上限，针对轮数r较小时，二者差别不大，甚至部分轮数是相等的. 文献[42]给出3个不同类CLEFIA动态密码结构最小差分活动轮函数的结果，如表2所示，证明本文推理的理论结果是正确的，不同轮的活动轮函数个数均小于上界. 而考虑6轮和12轮加密，CLEFIA密码结构活动轮函数个数和本文提出的动态密码结构轮函数上界均为6和12，即表明6轮和12轮加密，即使循环移位变化改为更复杂的GF(2^s)上动态线性变换，也无法提高相应的最小差分活动轮函数个数，文献[42]中3类动态密码结构验证了该结果. 因此，该理论有助于算法设计阶段从活动轮函数角度来平衡算法动态变化和轮数增加.

类似地，可将上述关于差分性质的结果推广到线

表2　四分支CLEFIA动态密码结构差分活动轮函数个数下界的比较

密码结构	轮数r									
	1	2	3	4	5	6	7	8	9	10
CLEFIA密码结构	0	1	2	3	4	6	6	7	8	9
I型类CLEFIA动态密码结构[42]	0	1	2	3	4	6	6	7	8	9
II型类CLEFIA动态密码结构[42]	0	1	2	3	4	6	6	7	8	9
一类CLEFIA动态密码结构[42]	0	1	2	3	4	6	6	7	8	9
动态密码结构上界	1	2	3	4	5	6	7	8	9	10
密码结构	轮数r									
	11	12	13	14	15	16	17	18	19	20
CLEFIA结构	10	12	12	13	14	15	16	18	18	19
I型类CLEFIA动态密码结构[42]	10	12	12	13	14	15	16	18	18	19
II型类CLEFIA动态密码结构[42]	10	12	12	13	14	15	16	18	19	19
一类CLEFIA动态密码结构[42]	10	12	12	13	14	15	16	18	19	19
动态密码结构上界	11	12	13	14	16	17	18	19	20	21

性性质,并给出如下定理:

定理 5 $2m$ 分支类 CLEFIA 动态密码结构的最小线性活动轮函数个数$\leqslant\left\lfloor\frac{2^{2m-1}}{2^{2m}-1}mr\right\rfloor$,其中,$2m$ 为广义类 CLEFIA 的分支个数,r 表示轮数,P_i 为基于 GF(2^s) 上 $\{0,1\}$ 构成的动态线性变换.

5 结束语

本文对 $2m$ 分支类 CLEFIA 动态密码结构进行研究,证明了基于循环移位变换 $2m$ 分支类 CLEFIA 动态密码结构与 CLEFIA 密码结构的差分等价性,回答了关于文献[40]中的 2 个问题,有助于加深对类 CLEFIA 动态密码结构的认识. 另外证明关于 r 轮 $2m$ 分支类 CLEFIA 动态密码结构最小差分活动轮函数个数上界$\left\lfloor\frac{2^{2m-1}}{2^{2m}-1}mr\right\rfloor$,其中,每轮 P_i 为基于 GF(2^s) 上 $\{0,1\}$ 构成的动态线性变换. 与已有下界结果比较,对算法设计阶段平衡算法动态和算法轮数的选择具有重要指导意义.

参考文献

[1] DAEMEN J, RIJMEN V. AES proposal: Rijndael[EB/OL]. (1999-09-03) [2022-01-25]. https://www.math.u-bor-deaux.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 block cipher CLEFIA (extended abstract) [C]//International Workshop on Fast Software Encryption. Berlin: Springer, 2007: 181-195.

[4] BIHAM E,SHAMIR A. Differential cryptanalysis of DES-like cryptosystems[J]. Journal of Cryptology, 1991, 4(1): 3-72.

[5] MATSUI M. Linear cryptanalysis method for DES cipher [C]//Advances in Cryptology-EUROCRYPT 1993. Berlin: Springer, 1994: 386-397.

[6] MOUHA N, WANG Q J, GU D W, et al. Differential and linear cryptanalysis using mixed-integer linear programming[C]//International Conference on Information Security and Cryptology. Berlin: Springer, 2012: 57-76.

[7] MASSACCI F, MARRARO L. Logical cryptanalysis as a SAT problem[J]. Journal of Automated Reasoning, 2000, 24(1): 165-203.

[8] SUN S W, HU L, WANG P, et al. Automatic security evaluation and (related-key) differential characteristic search: Application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2014: 158-178.

[9] ZHOU C N, ZHANG W T, DING T Y, et al. Improving the MILP-based security evaluation algorithm against differential/linear cryptanalysis using a divide-and-conquer approach[J]. IACR Transactions on Symmetric Cryptology, 2019(4): 438-469.

[10] SASAKI Y, TODO Y. New impossible differential search tool from design and cryptanalysis aspects[M]// Lecture Notes in Computer Science. Cham: Springer, 2017: 185-215.

[11] XIANG Z J, ZHANG W T, BAO Z Z, et al. Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers[M]// Advances in Cryptology-ASIACRYPT 2016. Berlin: Springer, 2016: 648-678.

[12] SUN L, WANG W, WANG M Q. Automatic search of bit-based division property for ARX ciphers and word-based division property[C]//International Conference on the Theory and Application of Cryptology and Information Security. Cham: Springer, 2017: 128-157.

[13] TODO Y, ISOBE T, HAO Y L, et al. Cube attacks on non-blackbox polynomials based on division property[J]. IEEE Transactions on Computers, 2018, 67(12): 1720-1736.

[14] WANG S P, HU B, GUAN J, et al. MILP-aided method of searching division property using three subsets and applications[C]//International Conference on the Theory and Application of Cryptology and Information Security. Cham: Springer, 2019: 398-427.

[15] HAO Y L, LEANDER G, MEIER W, et al. Modeling for three-subset division property without unknown subset [C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer, 2020: 466-495.

[16] LI T, SUN Y. SuperBall: A new approach for MILP modelings of Boolean functions[J]. IACR Transactions on Symmetric Cryptology, 2022(3): 341-367.

[17] BELLINI E, GERAULT D, GRADOS J, et al. Boosting differential-linear cryptanalysis of ChaCha7 with MILP[J]. IACR Transactions on Symmetric Cryptology, 2023(2): 189-223.

[18] BEYNE T, CHEN Y L, DOBRAUNIG C, et al. Status update on elephant[EB/OL]. (2022-09-17) [2023-06-01]. https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptogra-

phy/documents/round-2/status-update-sep2020/Elephant_status-update-round-2.pdf.

[19] DOBRAUNIG C, EICHLSEDER M, MANGARD S, et al. NIST Update: ISAP v2.0[EB/OL]. (2022-09-30) [2023-06-01]. https://csrc.nist.gov/csrc/media/Projects/lightweight-cryptography/documents/finalist-round/status-up - dates/isap-update.pdf.

[20] BANIK S, CHARKRABORTI A, INOUE A, et al. GIFT-COFB final round updates[EB/OL]. (2022-09-30) [2023-06-01]. https://csrc.nist.gov/csrc/media/Projects/lightweight-cryptography/documents/finalist-round/status-updates/gift-cofb-update.pdf.

[21] WU H, HUANG T. Tiny AMBU update[EB/OL]. (2022-09-30)[2023-06-01]. https://csrc.nist.gov/csrc/media/Projects/lightweight-cryptography/documents/finalist-round/status-updates/tinyjambu-update.pdf.

[22] HELL M, JOHANSSON T, MAXIMOR A, et al. Grain-128AEAD-status document[EB/OL]. (2022-09-30) [2023-06-01]. https://csrc.nist.gov/CSRC/media/Projects/lightweight - cryptography/documents/round - 2/status-update-sep2020/Grain_128AEAD_status_document.pdf.

[23] DOBRAUNIG C, EICHLSEDER M, MENDEL F, et al. Status update on Ascon v1.2[EB/OL]. (2022-09-30) [2023-06-01]. https://csrc. nist. gov/csrc/media/Projects/lightweight-cryptography/documents/finalist-round/status-updates/ascon-update.pdf.

[24] BAO Z, CHAKRABORTI A, DATTA N, et al. PHOTONBeetle authenticated encryption and Hash family-updated on software implementations[EB/OL]. (2022-09-30) [2023-06-01]. https://csrc. nist. gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/status-update-sep2020/PHOTON-Beetle_software_update_18Sep2020.pdf.

[25] BEIERLE C, BIRYUKOV A, SANTOS L C, et al. An update on the LWC finalist sparkle[EB/OL]. (2022-09-30) [2023-06-01]. https://csrc. nist. gov/csrc/media/Projects/lightweight-cryptography/documents/finalist-round/status-updates/sparkle-update.pdf.

[26] DAEMEN J, HOFFERT S, MELLA S, et al. Xoodyak, a fnal update[EB/OL]. (2020-09-18) [2023-06-01]. https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/status-update-sep2020/Xoodyak-update.pdf.

[27] GUO C, IWATA T, KHAIRALLAH M, et al. Final-round updates on Romulus[EB/OL]. (2022-09-27)[2023-06-01].https://csrc.nist.gov/csrc/media/Projects/lightweight-cryptography/documents/finalist - round/status - updates/romulus-update.pdf.

[28] CHAKRABORTY B, DHAR C, NANDI M. Exact security analysis of ASCON[C]//Advances in Cryptology-ASIACRYPT 2023. Singapore: Springer Lecture Notes in Computer Science, 2023: 346-369.

[29] DOBRAUNING C, EICHLSEDER M, MENDEL F, et al. Ascon v1.2[EB/OL]. (2016-09-15) [2023-06-01]. https://ascon.iaik.tugraz.at/files/asconv12.pdf.

[30] ADAMS C, GILCHRIST J. The CAST-256 encryption algorithm[J]. RFC, 1999, 2612: 1-19.

[31] FARAGALLAH O S, ELSAYED H, AFIFI A, et al. Small details gray scale image encryption using RC6 block cipher[J]. Wireless Personal Communications, 2021, 118: 1559-1589.

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

[33] BAO Z Z, GUO C, GUO J, et al. TNT: How to tweak a block cipher[M]//Advances in Cryptology - EUROCRYPT 2020. Cham: Springer International Publishing, 2020: 641-673.

[34] BANIK S, CHAKRABORTI A, IWATA T, et al. GIFT-COFB[P]. IACR Cryptology ePrint Archive, 2020: 738.

[35] BELLIZIA D, BERTI F, BRONCHAIN O, et al. Spook: Sponge-based leakage-resistant authenticated encryption with a masked tweakable block cipher[J]. IACR Transactions on Symmetric Cryptology, 2020(S1): 295-349.

[36] ZHENG Y L, MATSUMOTO T, IMAI H. On the construction of block ciphers provably secure and not relying on any unproved hypotheses[M]//Advances in Cryptology-CRYPTO' 89 Proceedings. New York: Springer, 2007: 461-480.

[37] SHIRAI T, SHIBUTANI K, AKISHITA T, et al. The 128-bit blockcipher CLEFIA (extended abstract) [M]//Fast Software Encryption. Berlin: Springer, 2007: 181-195.

[38] 郑建华, 任盛, 靖青, 等. Z密码算法设计方案[J]. 密码学报, 2018, 5(6): 579-590.
ZHENG J H, REN S, JING Q, et al. Z cipher scheme[J]. Journal of Cryptologic Research, 2018, 5(6): 579-590. (in Chinese)

[39] 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)

[40] 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)

[41] 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)

[42] 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)

[43] 沈璇, 刘国强, 孙兵, 等. 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[J]. 电子学报, 2024, 52(3): 709-718.
SHEN X, LIU G Q, SUN B, et al. Security evaluation against impossible differential cryptanalysis and zero correlation linear cryptanalysis for two dynamic cryptographic structures[J]. Acta Electronica Sinica, 2024, 52(3): 709-718. (in Chinese)

[44] 王念平, 洪礼荣. 类MARS密码结构的线性特性及其优化设计[J]. 通信学报, 2021, 42(4): 169-176.
WANG N P, HONG L R. Linear property and optimal design of MARS-like cryptographic structure[J]. Journal on Communications, 2021, 42(4): 169-176. (in Chinese)

作者简介

成 磊 男, 1988年11月出生, 江苏建湖人. 中国电子科技网络信息安全有限公司工程师, 电子科技大学计算机科学与工程学院博士后. 主要研究方向为密码学和信息安全.
E-mail: chenglei_1111@163.com

沈 璇 男, 1990年1月出生, 湖北荆门人. 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

任传伦 男, 1972年6月出生, 山东潍坊人. 中国电子科技集团公司第三十六研究所高级工程师. 主要研究方向为网络主动防御和信息安全.
E-mail: renchuanlun@gmail.com