类CLEFIA动态密码结构抵抗差分密码分析能力评估

杨继林,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: 将动态思想融入分组密码设计,使得算法具有动态性能从而提高抗攻击能力,按照这种想法,本文提出"类CLEFIA动态密码结构",并通过建立两类不同密码结构的差分对应之间的联系,给出类CLEFIA动态密码结构的差分密码分析结果.具体地,对$4r(r\geq 1)$轮类CLEFIA动态密码结构,在轮函数都是双射时,证明了$l(l\geq 1)$轮差分特征至少有l-1个活动轮函数.

关键词: 类CLEFIA动态密码结构; 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(2021)11-2279-05
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.12263/DZXB.20180973

Security Evaluation Against Differential Cryptanalysis for CLEFIA-like Dynamic Cryptographic Structure

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

Abstract: Based on the idea to integrate the dynamic idea into the block cipher design to make the algorithm have dynamic performance and to improve the anti-attack ability, CLEFIA-like dynamic cryptographic structure is put forward in this paper. By establishing the relation between differential correspondences of two classes of cryptographic structures, the ability of CLEFIA-like dynamic cryptographic structure to resist differential cryptanalysis is given. Concretely, for $4r(r\geq 1)$-round CLEFIA-like dynamic cryptographic structure, if the round functions are all bijective, then the number of active round functions for l-round differential characteristic is not less than l-1.

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

1 引言

目前,分组密码的应用越来越广泛.在长期的应用实践中,人们提出各种各样的分组密码结构[1],并利用这些结构设计了大量的分组密码算法.后来,有的学者提出将动态思想融入分组密码算法设计[2~12],使得算法具有动态性能,提高抗攻击能力,这就为分组密码算法的设计提供了一个较为新颖的思路.这里所说的"动态",是指分组密码算法的某些组件(例如S盒、扩散层或轮函数)有多种选择,或者说这些密码组件是动态可变的.但需要指出的是,这些融入动态思想的分组密码算法的抗攻击能力很大程度上依赖于所采用的分组密码结构的抗攻击能力,从而,对动态分组密码结构(即某些密码组件动态可变的分组密码结构)的研究就具有重要的意义.

另一方面,差分密码分析[13]是一种典型的分析方法,它主要考查明文对的差值在加密过程中的差分扩散特性.这种分析方法原来是针对DES[14]算法提出的,但后来的分析表明,这种分析方法适用于大多数分组密码,可以说,差分密码分析目前已成为人们重点考虑的攻击方法.基于此,本文提出一种动态分组密码结构,并对其抵抗差分密码分析的能力进行详细的研究.

顺便指出,本文提出的动态分组密码结构,特指分组密码结构每一轮中的块移位变换有两种选择,从而n轮动态分组密码结构中的块移位变换就有2^n种选择.每一种选择都对应一种分组密码结构,从而n轮动态分组密码结构就对应2^n种分组密码结构.这样,对动态分组密码结构进行分析,就相当于对多种分组密码结构进行分析;给出动态分组密码结构的差分密码分析结果,就相当于给出多种分组密码结构的差分密码分析

收稿日期:2018-11-07;修回日期:2021-10-06;责任编辑:郭游
基金项目:国家自然科学基金(No.61672031)

结果,从而更具有一般性的意义.

目前,人们对动态分组密码结构的研究,主要体现在以下几个方面:要么是对动态分组密码的设计方法和设计思想进行研究和分析[2~5],要么是针对具体的分组密码算法,将某些组件动态化,形成动态分组密码算法[6~12]. 其中,文献[2]提出可将一些密码组件作为动态可变因素设计动态分组密码算法,该文献以DES算法为例,将S盒作为动态可变因素,讨论了动态分组密码算法的实现方式. 文献[3]提出"对称密码算法簇模型",从混乱层和扩散层两个方面研究分组密码的动态组件设计问题,并基于AES、Camellia、SMS4算法给出了具体的密码算法簇,进而讨论了相应的硬件实现性能. 文献[6~8]对SMS4算法进行了改进,提出一种基于动态思想的SMS4算法,并从安全性和效率两方面对SMS4算法和其改进算法进行了对比分析. 总体来讲,除了上述文献[4,5]中的相应结果外,针对动态分组密码结构本身的研究却没有太多的结果.

2 预备知识

首先介绍CLEFIA密码结构和一类变形密码结构.

图1所示的是CLEFIA密码结构[15],它有4条输入分支x_0,x_1,x_2,x_3和4条输出分支y_0,y_1,y_2,y_3,每一轮中有两个轮函数f_0和f_1,$k=(k_0,k_1)$表示轮密钥,"⊕"表示异或运算,块移位变换P_i可以是变换$(a,b,c,d)\to(b,c,d,a)$(即循环左移变换),也可以是变换$(a,b,c,d)\to(d,a,b,c)$(即循环右移变换).

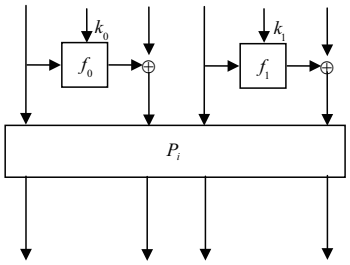


图1 CLEFIA密码结构

图2所示的是一类变形密码结构,它是在图1所示的CLEFIA密码结构的块移位变换之后加入2个异或运算.

下面介绍类CLEFIA动态密码结构.

$4r(r\geq 1)$轮类CLEFIA动态密码结构,它由r个"单元"$G_1,G_2,\cdots,G_r$迭代而成. 其中,任一"单元"$G_i(1\leq i\leq r$,即第$4i-3$轮至第$4i$轮)由4轮密码结构构成:前3轮是如图1所示的CLEFIA密码结构,第4轮是如图2所示的变形密码结构. 对任一"单元"$G_i(1\leq i\leq r)$,每一轮中的块移位变换可以是变换$(a,b,c,d)\to(b,c,d,a)$(即循环左移变换),也可以是变换$(a,b,c,d)\to(d,a,b,c)$(即循环右移变换),即每一轮中的块移位变换动态可变. 块移位变换的动态可变,就形成"$4r(r\geq 1)$轮类CLEFIA动态密码结构". 显然,每一轮中的块移位变换有2种选择:循环左移变换和循环右移变换,从而$4r$轮类CLEFIA动态密码结构中的块移位变换就有2^{4r}种选择,每一种选择都对应一种$4r$轮密码结构,故$4r$轮类CLEFIA动态密码结构就对应2^{4r}种$4r$轮密码结构.

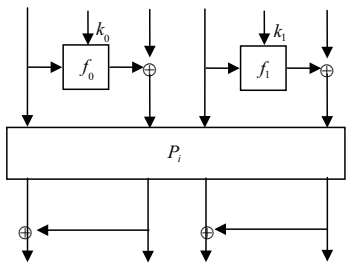


图2 一类变形密码结构

需要强调的是,$4r(r\geq 1)$轮类CLEFIA动态密码结构中,每一轮并不都是如图2所示的变形密码结构. 实际上,只有第4轮、第8轮、…、第$4r(r\geq 1)$轮是如图2所示的变形密码结构,而其它轮都是如图1所示的CLEFIA密码结构.

特别地,在$4r$轮类CLEFIA动态密码结构中,若每一轮中的块移位变换都是变换$(a,b,c,d)\to(b,c,d,a)$(即循环左移变换),则称该$4r$轮密码结构为"$4r$轮类CLEFIA密码结构"[16]. 换句话说,在$4r$轮类CLEFIA密码结构中,每一轮中的块移位变换都是变换$(a,b,c,d)\to(b,c,d,a)$(即循环左移变换).

定义1[17] 设$(X,+)$和$(Y,+)$都是有限交换群,f:$X\to Y,\alpha\in X,\beta\in Y$,差分概率$p_f(\alpha\to\beta)$定义为

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

这里,"+"表示群$(X,+)$中的群运算,$|X|$和$\#\{\bullet\}$表示基数.

定义2[18] 称输入差分非零的轮函数(包括f_0和f_1)为活动轮函数.

定义3 差分特征中活动轮函数的个数称为该差分特征的活动指标.

引理1 设$\alpha=(\alpha_0,\alpha_1,\alpha_2,\alpha_3),\beta=(\beta_0,\beta_1,\beta_2,\beta_3)$,则$\alpha\to\beta$是CLEFIA密码结构的1轮差分对应,当且仅当对$\forall l_1\in\{0,1\}$,存在$l_2\in\{0,1\}$,使得$(\alpha<<<2l_1)\to(\beta<<<2l_2)$是图1中块移位变换取循环左移变换时的密码结构的1轮差分对应. 此时,差分对应$\alpha\to\beta$和$(\alpha<<<2l_1)\to(\beta<<<2l_2)$的活动指标相等. 其中,$y<<<2x$表示$y=(y_0,y_1,y_2,y_3)$循环左移$2x$块,当$x=0$时,$y<<<2x=$

(y_0,y_1,y_2,y_3);当$x=1$时,$y<<<2x=(y_2,y_3,y_0,y_1)$.

证明　易知,图1中块移位变换取循环左移变换时,1轮差分对应都具有形式

$$(\alpha_0,\alpha_1,\alpha_2,\alpha_3)\to(\alpha_1\oplus\gamma_0,\alpha_2,\alpha_3\oplus\gamma_2,\alpha_0)\qquad(1)$$

且相应轮函数f_0和f_1的差分对应依次为$\alpha_0\to\gamma_0$和$\alpha_2\to\gamma_2$.

图1中块移位变换取循环右移变换时,1轮差分对应都具有形式

$$(\alpha_0,\alpha_1,\alpha_2,\alpha_3)\to(\alpha_3\oplus\gamma_2,\alpha_0,\alpha_1\oplus\gamma_0,\alpha_2)\qquad(2)$$

且相应轮函数f_0和f_1的差分对应依次为$\alpha_0\to\gamma_0$和$\alpha_2\to\gamma_2$.

在图1所示的CLEFIA密码结构中,块移位变换是在循环左移变换$(a,b,c,d)\to(b,c,d,a)$和循环右移变换$(a,b,c,d)\to(d,a,b,c)$中选取的,因此可分以下两种情形进行讨论.

情形1　图1所示的CLEFIA密码结构中的块移位变换取循环左移变换.

这时候,由式(1),不妨设$\beta=(\beta_0,\beta_1,\beta_2,\beta_3)=(\alpha_1\oplus\gamma_0,\alpha_2,\alpha_3\oplus\gamma_2,\alpha_0)$,则差分对应$\alpha\to\beta$就是$(\alpha_0,\alpha_1,\alpha_2,\alpha_3)\to(\alpha_1\oplus\gamma_0,\alpha_2,\alpha_3\oplus\gamma_2,\alpha_0)$,差分对应$(\alpha<<<2)\to(\beta<<<2)$就是$(\alpha_2,\alpha_3,\alpha_0,\alpha_1)\to(\alpha_3\oplus\gamma_2,\alpha_0,\alpha_1\oplus\gamma_0,\alpha_2)$. 再由式(1)知,$(\alpha_0,\alpha_1,\alpha_2,\alpha_3)\to(\alpha_1\oplus\gamma_0,\alpha_2,\alpha_3\oplus\gamma_2,\alpha_0)$是图1中块移位变换取循环左移变换时的密码结构的1轮差分对应当且仅当相应轮函数f_0和f_1的差分对应依次为$\alpha_0\to\gamma_0$和$\alpha_2\to\gamma_2$,同时,$(\alpha_2,\alpha_3,\alpha_0,\alpha_1)\to(\alpha_3\oplus\gamma_2,\alpha_0,\alpha_1\oplus\gamma_0,\alpha_2)$是图1中块移位变换取循环左移变换时的密码结构的1轮差分对应当且仅当相应轮函数f_0和f_1的差分对应依次为$\alpha_0\to\gamma_0$和$\alpha_2\to\gamma_2$,故$\alpha\to\beta$是图1中块移位变换取循环左移变换时的密码结构的1轮差分对应当且仅当$\alpha\to\beta$和$(\alpha<<<2)\to(\beta<<<2)$都是图1中块移位变换取循环左移变换时的密码结构的1轮差分对应.

这样就证明了:对$l_1=0$,存在$l_2=0$,使得$(\alpha<<<2l_1)\to(\beta<<<2l_2)$是图1中块移位变换取循环左移变换时的密码结构的1轮差分对应;对$l_1=1$,存在$l_2=1$,使得$(\alpha<<<2l_1)\to(\beta<<<2l_2)$是图1中块移位变换取循环左移变换时的密码结构的1轮差分对应. 显然,差分对应$\alpha\to\beta$和$(\alpha<<<2l_1)\to(\beta<<<2l_2)$的活动指标相等,该情形下定理结论成立.

情形2　图1所示的CLEFIA密码结构中的块移位变换取循环右移变换.

这时候,由式(2),不妨设$\beta=(\beta_0,\beta_1,\beta_2,\beta_3)=(\alpha_3\oplus\gamma_2,\alpha_0,\alpha_1\oplus\gamma_0,\alpha_2)$,则差分对应$\alpha\to\beta$就是$(\alpha_0,\alpha_1,\alpha_2,\alpha_3)\to(\alpha_3\oplus\gamma_2,\alpha_0,\alpha_1\oplus\gamma_0,\alpha_2)$,$\alpha\to(\beta<<<2)$就是$(\alpha_0,\alpha_1,\alpha_2,\alpha_3)\to(\alpha_1\oplus\gamma_0,\alpha_2,\alpha_3\oplus\gamma_2,\alpha_0)$,$(\alpha<<<2)\to\beta$就是$(\alpha_2,\alpha_3,\alpha_0,\alpha_1)\to(\alpha_3\oplus\gamma_2,\alpha_0,\alpha_1\oplus\gamma_0,\alpha_2)$. 由式(2)知,$(\alpha_0,\alpha_1,\alpha_2,\alpha_3)\to(\alpha_3\oplus\gamma_2,\alpha_0,\alpha_1\oplus\gamma_0,\alpha_2)$是图1中块移位变换取循环右移变换时的密码结构的1轮差分对应当且仅当相应轮函数f_0和f_1的差分对应依次为$\alpha_0\to\gamma_0$和$\alpha_2\to\gamma_2$. 再由式(1)知,$(\alpha_0,\alpha_1,\alpha_2,\alpha_3)\to(\alpha_1\oplus\gamma_0,\alpha_2,\alpha_3\oplus\gamma_2,\alpha_0)$是图1中块移位变换取循环左移变换时的密码结构的1轮差分对应当且仅当相应轮函数f_0和f_1的差分对应依次为$\alpha_0\to\gamma_0$和$\alpha_2\to\gamma_2$,并且$(\alpha_2,\alpha_3,\alpha_0,\alpha_1)\to(\alpha_3\oplus\gamma_2,\alpha_0,\alpha_1\oplus\gamma_0,\alpha_2)$是图1中块移位变换取循环左移变换时的密码结构的1轮差分对应当且仅当相应轮函数f_0和f_1的差分对应依次为$\alpha_0\to\gamma_0$和$\alpha_2\to\gamma_2$,故$\alpha\to\beta$是图1中块移位变换取循环右移变换时的密码结构的1轮差分对应当且仅当$\alpha\to(\beta<<<2)$和$(\alpha<<<2)\to\beta$都是图1中块移位变换取循环左移变换时的密码结构的1轮差分对应.

这样就证明了:对$l_1=0$,存在$l_2=1$,使得$(\alpha<<<2l_1)\to(\beta<<<2l_2)$是图1中块移位变换取循环左移变换时的密码结构的1轮差分对应;对$l_1=1$,存在$l_2=0$,使得$(\alpha<<<2l_1)\to(\beta<<<2l_2)$是图1中块移位变换取循环左移变换时的密码结构的1轮差分对应. 显然,差分对应$\alpha\to\beta$和$(\alpha<<<2l_1)\to(\beta<<<2l_2)$的活动指标相等,该情形下定理结论成立.

综上,引理得证. 证毕

备注1　文献[5]中的引理5.2.3实际上就是引理1的必要性.

引理1实际上是说,图1所示的CLEFIA密码结构存在1轮差分对应$\alpha\to\beta$当且仅当图1中块移位变换取循环左移变换时的密码结构存在活动指标相等的1轮差分对应$(\alpha<<<2l_1)\to(\beta<<<2l_2)$,且保证差分对应$(\alpha<<<2l_1)\to(\beta<<<2l_2)$在块移位变换取循环左移变换时的密码结构的多轮迭代中能够"传递"下去.

引理2　记号同引理1,则$\alpha\to\beta$是图2所示的变形密码结构的1轮差分对应,当且仅当对$\forall l_1\in\{0,1\}$,存在$l_2\in\{0,1\}$,使得$(\alpha<<<2l_1)\to(\beta<<<2l_2)$是图2中块移位变换取循环左移变换时的密码结构的1轮差分对应. 此时,差分对应$\alpha\to\beta$和$(\alpha<<<2l_1)\to(\beta<<<2l_2)$的活动指标相等.

证明　由图2和图1知,$\alpha\to\beta$是图2所示的变形密码结构的1轮差分对应当且仅当$\alpha\to\beta\oplus(\beta_1,0,\beta_3,0)$是图1所示的CLEFIA密码结构的1轮差分对应. 而

$$\begin{aligned}(\beta<<<2l_2)&=[(\beta_0,\beta_1,\beta_2,\beta_3)<<<2l_2]\\&=(\beta_{2l_2},\beta_{(1+2l_2)\bmod4},\beta_{(2+2l_2)\bmod4},\beta_{(3+2l_2)\bmod4})\\&\quad(\beta<<<2l_2)\oplus(\beta_{(1+2l_2)\bmod4},0,\beta_{(3+2l_2)\bmod4},0)\\&=(\beta<<<2l_2)\oplus[(\beta_1,0,\beta_3,0)<<<2l_2]\\&=[\beta\oplus(\beta_1,0,\beta_3,0)]<<<2l_2\end{aligned}$$

其中，$x \bmod 4$ 表示 4 除 x 的非负余数. 故由图 2 和图 1 知，$(\alpha <<< 2l_1) \rightarrow (\beta <<< 2l_2)$ 是图 2 中块移位变换取循环左移变换时的密码结构的 1 轮差分对应当且仅当 $(\alpha <<< 2l_1) \rightarrow [(\beta \oplus (\beta_1, 0, \beta_3, 0)) <<< 2l_2]$ 是图 1 中块移位变换取循环左移变换时的密码结构的 1 轮差分对应. 再由引理 1 知，$\alpha \rightarrow \beta \oplus (\beta_1, 0, \beta_3, 0)$ 是图 1 所示的 CLEFIA 密码结构的 1 轮差分对应当且仅当对 $\forall l_1 \in \{0, 1\}$，存在 $l_2 \in \{0, 1\}$，使得 $(\alpha <<< 2l_1) \rightarrow [(\beta \oplus (\beta_1, 0, \beta_3, 0)) <<< 2l_2]$ 是图 1 中块移位变换取循环左移变换时的密码结构的 1 轮差分对应.

综上，引理得证. 证毕

引理 3[16] 对 $4r(r \geq 1)$ 轮类 CLEFIA 密码结构，若轮函数都是双射，则 $l(1 \leq l \leq 4r)$ 轮差分特征的活动指标 $\geq l - 1$.

易知，差分概率 $p_f((0, 0, 0, 0) \rightarrow (0, 0, 0, 0)) = 1$. 这时候，称差分对应 $(0, 0, 0, 0) \rightarrow (0, 0, 0, 0)$ 为平凡的，否则称为非平凡的. 本文以下考虑的类 CLEFIA 动态密码结构的差分对应，都是非平凡的.

3 类 CLEFIA 动态密码结构抵抗差分密码分析的能力

在以下的研究中，假设类 CLEFIA 动态密码结构的轮函数 f_0 和 f_1 都是双射.

定理 1 对 $4r(r \geq 1)$ 轮类 CLEFIA 动态密码结构，设 C 表示该动态密码结构对应的 2^{4r} 种 $4r$ 轮密码结构中的任一种. 若轮函数都是双射，则 C 的 $l(1 \leq l \leq 4r)$ 轮差分特征的活动指标 $\geq l - 1$.

证明 用 C' 表示 $4r(r \geq 1)$ 轮类 CLEFIA 动态密码结构中的块移位变换都取循环左移变换时的密码结构，即 $4r(r \geq 1)$ 轮类 CLEFIA 密码结构. 由引理 1 和引理 2 知，C 有一条 l 轮差分特征当且仅当 C' 有一条活动指标相等的 l 轮差分特征，再由引理 3 知，C' 的活动指标 $\geq l - 1$，从而 C 的活动指标 $\geq l - 1$. 证毕

由定理 1，可得定理 2.

定理 2 对 $4r(r \geq 1)$ 轮类 CLEFIA 动态密码结构，设 C 表示该动态密码结构对应的 2^{4r} 种 $4r$ 轮密码结构中的任一种，若轮函数都是双射且最大差分概率为 $p_{\max}$，则 C 的 $l(1 \leq l \leq 4r)$ 轮差分特征概率 $\leq \left[p_{\max}\right]^{4k-1}$.

4 本文结论

本文提出了类 CLEFIA 动态密码结构，该动态密码结构对应多种分组密码结构，当迭代轮数较多时，直接对其进行差分密码分析是比较困难的. 本文通过分析 CLEFIA 密码结构和块移位变换取循环左移变换时的密码结构的差分对应之间的关系，在轮函数都是双射的条件下，给出了多种密码结构的差分密码分析结果. 本文的研究结果，对分组密码的设计与分析具有较大的指导意义[19~21]，但类 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它的线性变换时，是否有类似的结论成立？这些问题都值得进一步研究.

参考文献

[1] 吴文玲, 等. 分组密码的设计与分析(第二版)[M]. 北京: 清华大学出版社, 2009. 220 − 224.
WU Wen-ling, et al. Design and Analysis of Block Cipher (The Second Edition) [M]. Beijing: Tsinghua University Press, 2009. 220 − 224. (in Chinese)

[2] 胡祥义, 刘彤. 动态对称密码算法的研究与探讨[J]. 网络安全技术与应用, 2006, (3): 69 − 71.
HU Xiang-yi, LIU Tong. The research of dynamic symmetric cipher algorithm[J]. Network Security Technology & Application, 2006, (3): 69 − 71. (in Chinese)

[3] 杨宏志. 对称密码算法簇设计及其仿真[D]. 郑州: 解放军信息工程大学, 2010.
YANG Hong-zhi. Research on the design and simulation of symmetric cipher cluster[D]. Zhengzhou: The PLA Information Engineering University, 2010. (in Chinese)

[4] 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 Nian-ping. Security evaluation against differential cryptanalysis for four-block CLEFIA-like transform cluster [J]. Acta Electronica Sinica, 2017, 45(10): 2528 − 2532. (in Chinese)

[5] 殷勍. 几类分组密码结构抵抗差分和线性分析安全性研究[D]. 郑州：解放军信息工程大学, 2016.
YIN Qing. On security of several structures for block cipher against differential and linear cryptanalysis[D]. Zhengzhou: The PLA Information Engineering University, 2016. (in Chinese)

[6] 蒋继娅, 刘彤, 胡祥义. 动态 SMS4 算法的研究与实现[J]. 网络安全技术与应用, 2008, (9): 92 − 93.
JIANG Ji-ya, LIU Tong, HU Xiang-yi. Research and implementation of dynamic SMS4 algorithm[J]. Network Security Technology & Application, 2008, (9): 92 − 93. (in Chinese)

[7] 周术洋, 彭蔓蔓, 肖小欢. 一种基于动态思想的 SMS4 算法改进与实现[J]. 微电子学与计算机, 2011, 28(9): 86 − 88, 92.
ZHOU Shu-yang, PENG Man-man, XIAO Xiao-huan. An improvement of SMS4 algorithm based on dynamic ideas

[J]. Microelectronics & Computer, 2011, 28(9): 86 − 88,92. (in Chinese)

[8] 周术洋. 基于动态思想的SMS4算法研究[D]. 长沙:湖南大学, 2011.
ZHOU Shu-yang. An improvement of SMS4 algorithm based on dynamic ideas[D]. Changsha: Hunan University, 2011. (in Chinese)

[9] 李瑛, 胡祥义, 吕述望. 基于S盒编制的动态DES算法[J]. 计算机工程,2005, 31(23): 124 − 126.
LI Ying, HU Xiang-yi, LV Shu-wang. Dynamic DES based on S list [J]. Computer Engineering, 2005, 31(23): 124 − 126. (in Chinese)

[10] 陈利科, 张润彤. 一种基于动态S-盒P-盒的快速分组密码算法-DSP[J]. 计算机科学, 2009, 36(2): 78 − 81.
CHEN Li-ke, ZHANG Run-tong. Novel software block cipher using dynamic S-box and P-box[J]. Computer Science, 2009, 36(2): 78 − 81. (in Chinese)

[11] ZHAO Guosheng, WANG Jian. Security analysis and enhanced design of a dynamic block cipher[J]. China Communications, 2016, 13(1): 150 − 160.

[12] 赵国生, 李光程, 王健. 基于多维动态S盒和LFSR的分组密码算法[J]. 华中科技大学学报(自然科学版), 2015, 43(5): 119 − 123.
ZHAO Guo-sheng, LI Guang-cheng, WANG Jian. Block cipher algorithm based on multidimensional dynamic S-box and LFSR[J]. Journal of Huazhong University of Science and Technology(Natural Science Edition), 2015, 43 (5): 119 − 123. (in Chinese)

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

[14] NBS. Data encryption standard[S]. FIPS PUB 46, National Bureau of Standards, 1977.

[15] Shirai T, Shibutani K, Akishita T, et al. The 128-bit blockcipher CLEFIA[A]. Proceedings of the 14th International Workshop, FSE 2007[C]. Luxembourg, Luxembourg: Springer-Verlag, 2007. 181 − 195.

[16] 杨继林, 王念平. 类CLEFIA密码结构抵抗差分密码分析能力评估[J]. 密码与信息安全学报, 2018, 30(5): 7 − 11.
YANG Ji-lin, WANG Nian-ping. Security evaluation against differential cryptanalysis for CLEFIA-like cryptographic structure[J]. Journal of Cryptology and Information Security, 2018, 30(5): 7 − 11. (in Chinese)

[17] 金晨辉,郑浩然,张少武,等. 密码学[M]. 北京:高等教育出版社, 2009.175 − 176.
JIN Chen-hui, ZHENG Hao-ran, ZHANG Shao-wu, et al. Cryptology[M]. Beijing: Higher Education Press, 2009. 175 − 176. (in Chinese)

[18] Schneier B, Kelsey J. Unbalanced Feistel networks and block cipher design[A]. Proceedings of the 3rd International Workshop, FSE 1996[C]. Cambridge, UK: Springer-Verlag, 1996. 121−144.

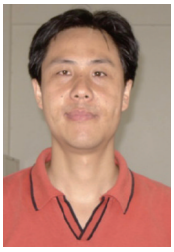
[19] 殷勍, 王念平. Piccolo结构抵抗差分和线性密码分析能力评估[J]. 山东大学学报(理学版), 2016, 51(3): 132 − 142.
YIN Qing, WANG Nian-Ping. Security evaluation for Piccolo structure against differential and linear cryptanalysis[J]. Journal of Shandong University(Natural Science), 2016, 51(3): 132 − 142. (in Chinese)

[20] 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 Nian-ping, YIN Qing. Security evaluation for SMS4-typed ciphers structure against differential and linear cryptanalysis[J]. Journal of Cryptologic Research, 2015, 2(2): 189 − 196. (in Chinese)

[21] 殷勍, 王念平. 一类扩展广义Feistel结构的活动轮函数个数的下界[J]. 河南师范大学学报(自然科学版), 2015, 43(5):142 − 146.
YIN Qing, WANG Nian-ping. Lower bounds on the number of active round functions for a class of extended generalized Feistel structure[J]. Journal of Henan Normal University (Natural Science Edition), 2015, 43(5): 142 − 146. (in Chinese)

作者简介

杨继林　男,1986年10月出生,江苏连云港人.2008年毕业于沈阳理工大学信息与计算科学专业,2017年进入解放军信息工程大学,2019年获密码学专业硕士学位,从事分组密码的设计与分析方面的有关研究.
E-mail:15245762243@163.com



王念平(通信作者)　男,1973年6月出生,河南洛阳人.博士、教授、博士生导师.分别于2001年、2008年在解放军信息工程大学获硕士、博士学位.主要从事密码学和信息安全等方面的研究工作.
E-mail:wwnnpp@126.com