动态密码结构抵抗差分密码分析能力评估

王念平，郭祉成
（信息工程大学，河南 郑州 450001）

摘 要：针对 CLEFIA 密码结构，提出一种动态密码结构，该动态密码结构的特点是第 $6t(t\geq 1)$轮中的扩散层可以从 $\{0,1\}^4$ 上的多个线性双射中任意选取。通过对 6 轮差分特征的传递规律的分析，给出了动态密码结构中所有密码结构抵抗差分密码分析能力的评估结果。研究结果表明，在轮函数都是双射的条件下，当迭代轮数 l 为 $6k(k\geq 1)$或 $6k+1(k\geq 3)$时，l 轮差分特征至少有 l 个活动轮函数，当迭代轮数为其他值时，l 轮差分特征至少有 $l-1$ 个活动轮函数。

关键词：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
DOI: 10.11959/j.issn.1000−436x.2021112

Security evaluation against differential cryptanalysis for dynamic cryptographic structure

WANG Nianping, GUO Zhicheng
Information Engineering University, Zhengzhou 450001, China

Abstract: For CLEFIA cryptographic structure, a dynamic cryptographic structure was put forward. The main feature of the dynamic cryptographic structure was that the diffusion layer in the $6t(t\geq 1)$th round could be selected arbitrarily from some linear bijection on $\{0,1\}^4$. By analysing the transfer law of 6-round differential characteristic, security evaluation against differential cryptanalysis for all structures of the dynamic cryptographic structure was given. The results show that, under the condition that the round functions are all bijective, there are at least l active round functions for l-round differential characteristic when l is $6k(k\geq 1)$ or $6k+1(k\geq 3)$, and otherwise there are at least $l-1$ active round functions for l-round differential characteristic.

Keywords: dynamic cryptographic structure, differential cryptanalysis, active round function

1 引言

随着分组密码研究的不断深入，一些学者为了提高分组密码算法的安全性，提出了动态分组密码算法[1-10]，这就为分组密码算法的设计提供了一条新的思路。“动态”是指分组密码算法的某些组件（例如 S 盒、扩散层或轮函数等）有多种选择，或者说这些密码组件是动态可变的。但必须指出，这些动态分组密码算法的抗攻击能力很大程度上取决于所采用的分组密码结构的抗攻击能力，因此，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）的研究具有重要的意义。

另一方面，差分密码分析[11]是攻击分组密码最有效的方法之一，对分组密码抵抗差分密码分析的能力进行评估一直都是密码学研究的热点。如果分组密码的最大差分特征概率足够小，就可以认为该分组密码能够抵抗差分密码分析。在评估分组密码抵抗差分密码分析的能力时，研究方法通常是给出多轮差分特征中活动轮函数或活动 S 盒个数的下界，进而给出最大差分特征概率的上界。

一般来说，将分组密码结构的某些组件（例如 S 盒、扩散层或轮函数等）动态化，就可以构成动

收稿日期：2021−01−20；**修回日期**：2021−04−06
基金项目：国家自然科学基金资助项目（No.61672031）
Foundation Item: The National Natural Science Foundation of China (No.61672031)

态分组密码结构，但如果这些组件设计不当，就有可能导致动态分组密码结构中的某些密码结构抗攻击能力较弱。这样，密码分析者就有可能针对这一较弱的结构进行攻击，从而带来意想不到的后果。因此，在设计动态分组密码结构时，一定要尽量保证动态密码结构中的任一结构具有相同或相近的抗攻击能力，避免出现某一结构抗攻击能力较弱的情况。

基于上述的想法，本文根据差分传递规律，提出一种动态密码结构，并对其抵抗差分密码分析的能力进行了详细的评估，给出了多轮差分特征中活动轮函数个数的下界。该动态密码结构的特点是第 $6t(\forall t \geqslant 1)$ 轮中的扩散层可以从 $\{0,1\}^4$ 上的多个线性双射（对应于 4 阶 0-1 可逆矩阵）中任意选取，即 $6t(\forall t \geqslant 1)$ 轮中的扩散层是动态可变的。这里所说的“扩散层”是指整体结构中的扩散层，而不是轮函数中的扩散层。需要强调的是，本文提出的动态密码结构中的扩散层并不是随意选取的，也并非涵盖所有的 4 阶 0-1 可逆矩阵，而是根据差分传递规律设计的。扩散层的设计是本文的创新之处，给出多轮差分特征中活动轮函数个数的下界是本文首要解决的问题。

目前，与动态分组密码结构有关的研究主要有以下 2 个方面。1) 对动态分组密码的设计思想和设计方法进行研究和探讨[1-3,12-19]。文献[1]设计了一种嵌套复用 S 盒的动态密码算法，为不同用户提供不同的分组密码算法。文献[2]通过变换对称密码算法中的编制要素，实现动态对称密码算法。文献[3]提出“对称密码算法簇模型”，从混乱层和扩散层 2 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[12-16]对几类动态分组密码结构的设计方法以及抵抗差分或线性密码分析的能力进行了分析。文献[17-19]通过选取不同的扩散矩阵，提升了密码算法中活动轮函数个数的下界，提高了密码算法抵抗差分或者线性密码分析能力。2) 针对具体的分组密码算法，将某些密码组件动态化，形成动态分组密码算法[4-10]。文献[4-6]基于 SMS4 算法，利用时间戳动态改变算法中的固定参数，从而实现密码算法的动态化。文献[7,9-10]利用密钥控制动态可变的 S 盒，能够使密码算法动态可变。文献[8]基于 Feistel 结构，设计了结合密钥相关的动态 S 盒和 P 盒，提出了一种动态分组密码算法。除了文献[12-16]中的相应结果外，大多工作都是针对具体的密码算法中的组件（如 S 盒、P 盒、某个参数等）进行研究的，针对动态分组密码结构本身的研究并不多。本文提出的动态密码结构与以上所述的这些研究都有所不同，因此本文的研究具有重要的意义。此外，动态分组密码结构的安全性研究对动态分组密码设计与分析具有重要的指导意义，可以根据本文提出的动态密码结构设计出相应的动态分组密码算法。本文对该动态密码结构进行抵抗差分密码分析，其分析结果可以保证基于该结构设计的动态分组密码算法抵抗差分密码分析的安全性，并为动态分组密码算法设计提供了一定的依据。

2　预备知识

CLEFIA 密码结构如图 1 所示，它有 4 个输入分支 (x_0,x_1,x_2,x_3) 和 4 个输出分支 (y_0,y_1,y_2,y_3)，每一轮中有 2 个轮函数 f_0 和 f_1，线性变换采用循环左移变换，其中 $k=(k_0,k_1)$ 表示轮密钥，$\oplus$ 表示异或运算。

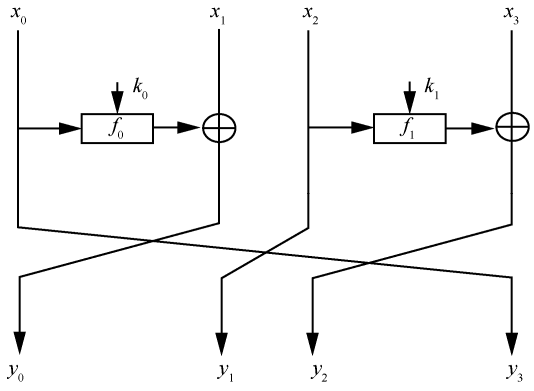


图 1　CLEFIA 密码结构

CLEFIA 变形密码结构如图 2 所示，其主要特点是线性变换 $\boldsymbol{P}$（即扩散层）可以从形如 $\boldsymbol{P}_1=\begin{pmatrix}0&1&0&1\\0&\lambda_0&1&\lambda_1\\0&0&0&1\\1&\lambda_2&\lambda_3&\lambda_4\end{pmatrix}$ 或 $\boldsymbol{P}_2=\begin{pmatrix}0&1&0&1\\1&\mu_0&\mu_1&\mu_2\\0&0&0&1\\0&\mu_3&1&\mu_4\end{pmatrix}$ 的 4 阶 0,1 可逆矩阵中任意选取，其中 $\lambda_i,\mu_i\in\{0,1\}$，$0\leqslant i\leqslant 4$。显然，对任意给定的 $i,0\leqslant i\leqslant 4$，$\lambda_i$ 和 μ_i 都有 2 种选取方法（即 0 或 1），故线性变换 $\boldsymbol{P}$ 共有 $2^5\times 2=2^6$ 种选取方法。

由图 2 可知，CLEFIA 变形密码结构的输入与输出的关系式为

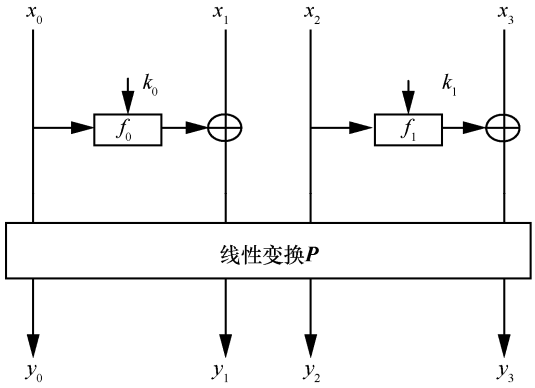


图 2 CLEFIA 变形密码结构

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

其中，$(x_0,f_0(x_0\oplus k_0)\oplus x_1,x_2,f_1(x_2\oplus k_1)\oplus x_3)\boldsymbol{P}$ 表示向量 $(x_0,f_0(x_0\oplus k_0)\oplus x_1,x_2,f_1(x_2\oplus k_1)\oplus x_3)$ 与矩阵 $\boldsymbol{P}$ 相乘。例如，当线性变换 $\boldsymbol{P}=\begin{pmatrix}0&1&0&1\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{pmatrix}$ 时，CLEFIA 变形密码结构的输入与输出的关系式为

$$Q_k(x_0,x_1,x_2,x_3)=(x_0,f_0(x_0\oplus k_0)\oplus$$
$$x_1,x_2,f_1(x_2\oplus k_1)\oplus x_3)\begin{pmatrix}0&1&0&1\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{pmatrix}=$$
$$(f_1(x_2\oplus k_1)\oplus x_3,x_0,f_0(x_0\oplus k_0)\oplus x_1,x_0\oplus x_2)$$

$6t+m(t\geqslant 0,0\leqslant m\leqslant 5)$ 轮基于 CLEFIA 变形密码结构的动态密码结构（以下简称动态密码结构）如图 3 所示，它由 t 个“单元” $G_i(1\leqslant i\leqslant t)$ 和 m 轮 CLEFIA 密码结构组成。其中任一“单元” G_i（即第 $6i-5$ 轮～第 $6i$ 轮，$1\leqslant i\leqslant t$，如图 4 所示）由 6 轮密码结构构成：前 5 轮是如图 1 所示的 CLEFIA 密码结构，第 6 轮是如图 2 所示的 CLEFIA 变形密码结构。也就是说，$6t+m$ 轮动态密码结构中，第 6 轮、第 12 轮、…、第 $6t$ 轮是如图 2 所示的 CLEFIA 变形密码结构，其他轮都是如图 1 所示的 CLEFIA 密码结构。需要强调的是，第 6 轮、第 12 轮、…、第 $6t$ 轮中的线性变换可以相同，也可以不同，换句话说，第 6 轮、第 12 轮、…、第 $6t$ 轮中的线性变换是独立选取的，故 $6t+m(t\geqslant 0,0\leqslant m\leqslant 5)$ 轮动态密码结构共包含 $(2^5\times 2)^t=2^{6t}$ 种密码结构。

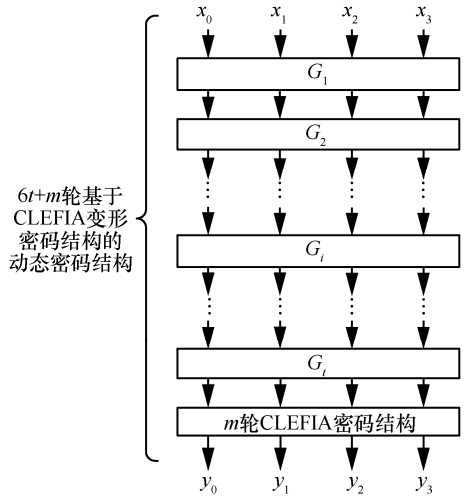


图 3 基于 CLEFIA 变形密码结构的动态密码结构

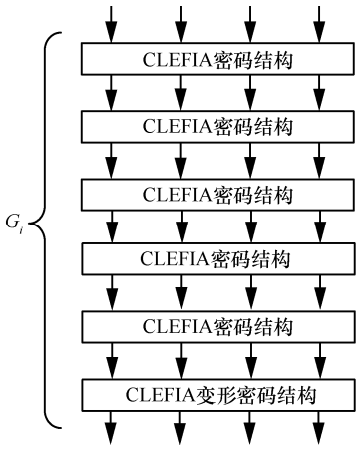


图 4 “单元” G_i

定义 1[20] 设 $(X,+)$ 和 $(Y,+)$ 都是有限交换群，$f:X\to Y$，$\alpha\in X$，$\beta\in Y$，令

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

则称 $p_f(\alpha\to\beta)$ 为 f 在输入差为 α 条件下，输出差为 β 的差分概率。此外，也称 $\alpha\to\beta$ 为 f 的一个差分对应，并称 $p_f(\alpha\to\beta)$ 为该差分对应的概率。其中“+”表示群 $(X,+)$ 中的运算，$|X|$ 和 $\#\{\cdot\}$ 都表示集合的元素个数。

定义 2[20] 设 $(X,+)$ 是有限交换群，$f_{k_1,\cdots,k_n}=f_{k_n}f_{k_{n-1}}\cdots f_{k_2}f_{k_1}$，$\alpha_1,\cdots,\alpha_{n+1}\in X$，则称 $\alpha_1\to\alpha_2\to\alpha_3\to\cdots\to\alpha_n\to\alpha_{n+1}$ 为 $f_{k_1,\cdots,k_n}$ 的一个起点为 α_1，终点为 α_{n+1} 的差分传递链。

在本文中，称 $\alpha_1\to\alpha_2\to\alpha_3\to\cdots\to\alpha_n\to\alpha_{n+1}$

为 n 轮差分特征，并称 $p_{f_{k_1}}(\alpha_1 \to \alpha_2)\ p_{f_{k_2}}(\alpha_2 \to \alpha_3)\cdots p_{f_{k_n}}(\alpha_n \to \alpha_{n+1})$ 为该差分特征的概率。

定义 3[21] 设 $\alpha \to \beta$ 是轮函数（包括 f_0 和 f_1）的一个差分对应，若 $\alpha \neq 0$，则称该轮函数是活动的，或称该轮函数是活动轮函数。

引理 1[16] 对于图 1 所示的 CLEFIA 密码结构，设轮函数都是双射，则 $r(r \geqslant 0)$ 轮差分特征至少有 $r - \lceil (r \bmod 6)/6 \rceil$ 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 CLEFIA 动态密码结构抵抗差分密码分析

为了方便研究，用 $\Delta X = (\Delta x_{4i}, \Delta x_{4i+1}, \Delta x_{4i+2}, \Delta x_{4i+3})$ 表示图 3 所示的动态密码结构的输入和输出差分 $(i \geqslant 0)$，同时假设轮函数 f_0 和 f_1 都为双射。这里，只考虑差分的输出规律，并不考虑差分的具体数值，因此可以将所有的差分块 $\Delta x_{4i}, \Delta x_{4i+1}, \Delta x_{4i+2}, \Delta x_{4i+3}$ 用“0”或“1”表示。其中，“0”表示 0 差分块，“1”表示非 0 差分块，于是非 0 输入差分和输出差分可以用 (0,0,0,1),(0,0,1,0), (0,0,1,1),⋯,(1,1,1,1) 表示，分别简记为 1,2,3,⋯,15。按照这种表示方法，差分块之间的运算为“0⊕0=0”“0⊕1=1”“1⊕0=1”“1⊕1=0 或 1”。其中，“1⊕1=0”表示 2 个非 0 差分块相等时的异或结果为 0 差分块，记为“0”；“1⊕1=1”表示 2 个非 0 差分块不相等时的异或结果为非 0 差分块，记为“1”。

首先，给出所有非 0 输入差分经一轮 CLEFIA 密码结构（如图 1 所示）迭代后的差分对应。

以输入差分为 $(0,0,1,1)=3$ 时的情形为例。此时，第 3 分支与第 4 分支输入差分不为 0，CLEFIA 密码结构的一轮差分对应为

$$3=(0,0,1,1) \xrightarrow{f_0, f_1, \oplus, \oplus} \begin{cases} (0,0,1,0) \\ (0,0,1,1) \end{cases} \xrightarrow{\text{循环左移}} \begin{cases} (0,1,0,0)=4 \\ (0,1,1,0)=6 \end{cases}$$

简记为

$$3 \xrightarrow{1(1)} 4,6$$

其中，箭头上方括号中的 1 表示轮函数 f_1 的输入差分块为非 0 差分块，即活动轮函数的个数为 1。以下都用 $\alpha \xrightarrow{u(v)} \beta (1 \leqslant \alpha, \beta \leqslant 15)$ 表示输入差分 α 经过 $u(u \geqslant 1)$ 轮迭代后输出差分为 β，且活动轮函数的个数为 v。

上述差分对应的计算过程如下：在轮函数 f_0 和 f_1 都为双射的条件下，当输入差分为 $3=(0,0,1,1)$ 时，轮函数 f_0 的输出差分块为 0 差分块，轮函数 f_1 的输出差分块为非 0 差分块，故由“0⊕0=0”和“1⊕1=0 或 1”知，经过轮函数 f_0 和 f_1 以及异或运算作用后，其输出结果为 (0,0,1,0) 或 (0,0,1,1)，再经过循环左移变换，其输出结果为 (0,1,0,0) 或 (0,1,1,0)，即 4 或 6。

类似地，所有非 0 输入差分经一轮 CLEFIA 密码结构迭代后的差分对应为

$1 \xrightarrow{1(0)} 2$　　$2 \xrightarrow{1(1)} 6$　　$3 \xrightarrow{1(1)} 4,6$

$4 \xrightarrow{1(0)} 8$　　$5 \xrightarrow{1(0)} 10$　　$6 \xrightarrow{1(1)} 14$

$7 \xrightarrow{1(1)} 12,14$　　$8 \xrightarrow{1(1)} 9$　　$9 \xrightarrow{1(1)} 11$

$10 \xrightarrow{1(2)} 15$　　$11 \xrightarrow{1(2)} 13,15$　　$12 \xrightarrow{1(1)} 1,9$

$13 \xrightarrow{1(1)} 3,11$　　$14 \xrightarrow{1(2)} 7,15$　　$15 \xrightarrow{1(2)} 5,7,13,15$

其次，给出所有非 0 输入差分经一轮 CLEFIA 变形密码结构（如图 2 所示）迭代后的差分对应。

当线性变换 $\boldsymbol{P} \in \boldsymbol{P}_1$ 时，以输入差分为 $(0,0,1,1)=3$ 时的情形为例。此时，第 3 分支与第 4 分支输入差分不为 0，CLEFIA 变形密码结构的一轮差分对应为

$$3=(0,0,1,1) \xrightarrow{f_0, f_1, \oplus, \oplus} \begin{cases} (0,0,1,0) \\ (0,0,1,1) \end{cases} \xrightarrow{P_1} \begin{cases} (0,0,0,1)=1 \\ (1,\lambda_2,\lambda_3,1\oplus\lambda_4) \end{cases}$$

其中，$\lambda_i \in \{0,1\}, 2 \leqslant i \leqslant 4$，且运算 $\oplus$ 满足规则“0⊕0=0”“0⊕1=1”“1⊕0=1”“1⊕1=0 或 1”。当 λ_i 遍历 0,1 时，$(1,\lambda_2,\lambda_3,1\oplus\lambda_4)$ 的取值为 $(1,0,0,1\oplus 0)=(1,0,0,1)$，$(1,0,0,1\oplus 1)=(1,0,0,0)$ 或 $(1,0,0,1)$，$(1,0,1,1\oplus 0)=(1,0,1,1)$，$(1,0,1,1\oplus 1)=(1,0,1,0)$ 或 $(1,0,1,1)$，$(1,1,0,1\oplus 0)=(1,1,0,1)$，$(1,1,0,1\oplus 1)=(1,1,0,0)$ 或 $(1,1,0,1)$，$(1,1,1,1\oplus 0)=(1,1,1,1)$，$(1,1,1,1\oplus 1)=(1,1,1,0)$ 或 $(1,1,1,1)$，即 $(1,\lambda_2,\lambda_3,1\oplus\lambda_4)$ 的取值 $\in \{8,9,10,11,12,13,14,15\}$，故上述的一轮差分对应可简记为

$$3 \xrightarrow{1(1)} 1,8,9,10,11,12,13,14,15$$

其中，箭头上方括号中的 1 表示轮函数 f_1 的输入差分块为非 0 差分块，即活动轮函数的个数为 1。

当线性变换 $\boldsymbol{P}\in\boldsymbol{P}_2$ 时，仍以输入差分为 $(0,0,1,1)=3$ 时的情形为例。同样可以给出输入差分 3 经一轮 CLEFIA 变形密码结构迭代后的差分对应为

$$3\xrightarrow{1(1)}1,2,3,6,7$$

利用上述的 $\boldsymbol{P}\in\boldsymbol{P}_1$ 和 $\boldsymbol{P}\in\boldsymbol{P}_2$ 时的差分对应，进一步可以给出当线性变换 $\boldsymbol{P}\in\boldsymbol{P}_1\cup\boldsymbol{P}_2$ 时，输入差分 3 经一轮 CLEFIA 变形密码结构迭代后的差分对应为

$$3\xrightarrow{1(1)}1,2,3,6,7,8,9,10,11,12,13,14,15$$

即将 $3\xrightarrow{1(1)}1,8,9,10,11,12,13,14,15$ 和 $3\xrightarrow{1(1)}1,2,3,6,7$ 进行合并。

类似地，所有非 0 输入差分经一轮 CLEFIA 变形密码结构迭代后的差分对应为

$$1\xrightarrow{1(0)}2,3,6,7,8,9,10,11,12,13,14,15$$

$$2\xrightarrow{1(1)}2,3,6,7,8,9,10,11,12,13,14,15$$

$$3\xrightarrow{1(1)}1,2,3,6,7,8,9,10,11,12,13,14,15$$

$$4\xrightarrow{1(0)}2,3,6,7,8,9,10,11,12,13,14,15$$

$$5\xrightarrow{1(0)}8,9,10,11,12,13,14,15$$

$$6\xrightarrow{1(1)}8,9,10,11,12,13,14,15$$

$$7\xrightarrow{1(1)}2,3,6,7,8,9,10,11,12,13,14,15$$

$$8\xrightarrow{1(1)}2,3,6,7,8,9,10,11,12,13,14,15$$

$$9\xrightarrow{1(1)}8,9,10,11,12,13,14,15$$

$$10\xrightarrow{1(2)}8,9,10,11,12,13,14,15$$

$$11\xrightarrow{1(2)}2,3,6,7,8,9,10,11,12,13,14,15$$

$$12\xrightarrow{1(1)}2,3,5,6,7,8,9,10,11,12,13,14,15$$

$$13\xrightarrow{1(1)}2,3,6,7,8,9,10,11,12,13,14,15$$

$$14\xrightarrow{1(2)}2,3,6,7,8,9,10,11,12,13,14,15$$

$$15\xrightarrow{1(2)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15$$

利用上述的一轮 CLEFIA 密码结构的差分对应和一轮 CLEFIA 变形密码结构的差分对应，可以进一步给出所有非 0 输入差分经 6 轮动态密码结构（如图 3 和图 4 所示）迭代后的差分对应为

$$1\begin{cases}\xrightarrow{6(6)}2,3,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(7)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(8)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\end{cases}$$

$$2\begin{cases}\xrightarrow{6(6)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(7)}8,9,10,11,12,13,14,15\\ \xrightarrow{6(8)}1,2,3,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(9)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(10)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\end{cases}$$

$$3\begin{cases}\xrightarrow{6(6)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(7)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(8)}1,2,3,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(9)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(10)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\end{cases}$$

$$4\begin{cases}\xrightarrow{6(6)}1,2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(7)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(8)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\end{cases}$$

$$5\begin{cases}\xrightarrow{6(6)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(7)}8,9,10,11,12,13,14,15\\ \xrightarrow{6(8)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(9)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(10)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\end{cases}$$

$$6\begin{cases}\xrightarrow{6(6)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(7)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(8)}1,2,3,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(9)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(10)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(11)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\end{cases}$$

$$7\begin{cases}\xrightarrow{6(6)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(7)}1,2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(8)}2,3,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(9)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(10)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(11)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\end{cases}$$

$$8\begin{cases}\xrightarrow{6(6)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(7)}8,9,10,11,12,13,14,15\\ \xrightarrow{6(8)}1,2,3,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(9)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(10)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\end{cases}$$

$$9\begin{cases}\xrightarrow{6(6)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(7)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(8)}1,2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(9)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(10)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(11)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\end{cases}$$

$$10\begin{cases}\xrightarrow{6(7)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(8)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(9)}1,2,3,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(10)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(11)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(12)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\end{cases}$$

$$11\begin{cases}\xrightarrow{6(6)}8,9,10,11,12,13,14,15\\ \xrightarrow{6(7)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(8)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(9)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(10)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(11)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(12)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\end{cases}$$

$$12\begin{cases}\xrightarrow{6(6)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(7)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(8)}1,2,3,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(9)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(10)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\end{cases}$$

$$13\begin{cases}\xrightarrow{6(6)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(7)}2,3,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(8)}1,2,3,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(9)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(10)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(11)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\end{cases}$$

$$14\begin{cases}\xrightarrow{6(6)}8,9,10,11,12,13,14,15\\ \xrightarrow{6(7)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(8)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(9)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(10)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(11)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(12)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\end{cases}$$

$$15\begin{cases}\xrightarrow{6(6)}8,9,10,11,12,13,14,15\\ \xrightarrow{6(7)}2,3,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(8)}2,3,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(9)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(10)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(11)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\\ \xrightarrow{6(12)}1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\end{cases}$$

由上面的讨论，可得以下引理。

引理 2　对于图 3 所示的动态密码结构，若轮函数都是双射，则有以下结论成立。

1) 6 轮差分特征中活动轮函数的个数≥6 。

2) 活动轮函数为 6 的 6 轮差分特征只可能为

$1\xrightarrow{6(6)}2,3,5,6,7,8,9,10,11,12,13,14,15$

$2\xrightarrow{6(6)}2,3,6,7,8,9,10,11,12,13,14,15$

$3\xrightarrow{6(6)}2,3,6,7,8,9,10,11,12,13,14,15$

$4\xrightarrow{6(6)}1,2,3,6,7,8,9,10,11,12,13,14,15$

$5\xrightarrow{6(6)}2,3,6,7,8,9,10,11,12,13,14,15$

$6\xrightarrow{6(6)}2,3,6,7,8,9,10,11,12,13,14,15$

$7\xrightarrow{6(6)}2,3,6,7,8,9,10,11,12,13,14,15$

$8\xrightarrow{6(6)}2,3,6,7,8,9,10,11,12,13,14,15$

$9\xrightarrow{6(6)}2,3,6,7,8,9,10,11,12,13,14,15$

$11\xrightarrow{6(6)}8,9,10,11,12,13,14,15$

$12\xrightarrow{6(6)}2,3,6,7,8,9,10,11,12,13,14,15$

$13\xrightarrow{6(6)}2,3,6,7,8,9,10,11,12,13,14,15$

$14\xrightarrow{6(6)}8,9,10,11,12,13,14,15$

$15\xrightarrow{6(6)}8,9,10,11,12,13,14,15$

引理 3　对于图 3 所示的动态密码结构，在轮函数都是双射的条件下，19 轮差分特征中活动轮函数的个数≥19，即对于

$$\Delta X^{(0)}\xrightarrow{6(v_1)}\Delta X^{(1)}\xrightarrow{6(v_2)}\Delta X^{(2)}\xrightarrow{6(v_3)}\Delta X^{(3)}\xrightarrow{1(v_4)}\Delta X^{(4)}\quad(1\leqslant\Delta X^{(i)}\leqslant 15,0\leqslant i\leqslant 4)$$

都有 $v_1+v_2+v_3+v_4\geqslant 19$ 。

证明　由引理 2 的 1)可知，6 轮差分特征中活动轮函数的个数≥6，故 $v_i\geqslant 6(1\leqslant i\leqslant 3)$。

情形 1　$\Delta X^{(3)}\neq 1,4,5$ 。

由 $\Delta X^{(3)}\neq 1,4,5$ 和一轮 CLEFIA 密码结构的差分对应可知 $v_4\geqslant 1$，因此 $v_1+v_2+v_3+v_4\geqslant 6+6+6+1=19$，即 $v_1+v_2+v_3+v_4\geqslant 19$ 。

情形 2 $\Delta X^{(3)}$=1,4,5。

当 $\Delta X^{(3)}=1$ 时，若 $v_3 \geqslant 7$，则 $v_1+v_2+v_3+v_4 \geqslant 6+6+7+0=19$，即 $v_1+v_2+v_3+v_4 \geqslant 19$；否则，由 $\Delta X^{(3)}=1$、$v_3=6$ 和引理 2 的 2)可知，$\Delta X^{(2)}$=4（即输出差分为 1 且活动轮函数个数为 6 的差分特征只可能为 $4 \xrightarrow{6(6)} 1,2,3,6,7,8,9,10,11,12,13,14,15$），由引理 2 的 2)可知，$v_2 \geqslant 7$（即不存在输出差分为 4 且活动轮函数个数为 6 的差分特征），因此 $v_1+v_2+v_3+v_4 \geqslant 6+7+6+0=19$，即 $v_1+v_2+v_3+v_4 \geqslant 19$。

当 $\Delta X^{(3)}=4$ 时，由引理 2 的 2)可知，$v_3 \geqslant 7$（即不存在输出差分为 4 且活动轮函数个数为 6 的差分特征），因此 $v_1+v_2+v_3+v_4 \geqslant 6+6+7+0=19$，即 $v_1+v_2+v_3+v_4 \geqslant 19$。

当 $\Delta X^{(3)}=5$ 时，若 $v_3 \geqslant 7$，则 $v_1+v_2+v_3+v_4 \geqslant 6+6+7+0=19$，即 $v_1+v_2+v_3+v_4 \geqslant 19$；若 $v_2 \geqslant 7$，则 $v_1+v_2+v_3+v_4 \geqslant 6+7+6+0=19$，即 $v_1+v_2+v_3+v_4 \geqslant 19$；否则，由 $\Delta X^{(3)}=5$、$v_2=v_3=6$ 和引理 2 的 2)可知，$\Delta X^{(2)}=1$，$\Delta X^{(1)}=4$（即输出差分为 5 且活动轮函数个数为 6 的差分特征只可能为 $1 \xrightarrow{6(6)} 2,3,5,6,7,8,9,10,11,12,13,14,15$，输出差分为 1 且活动轮函数个数为 6 的差分特征只可能为 $4 \xrightarrow{6(6)} 1,2,3,6,7,8,9,10,11,12,13,14,15$），由引理 2 的 2)可知 $v_1 \geqslant 7$（即不存在输出差分为 4 且活动轮函数个数为 6 的差分特征），因此 $v_1+v_2+v_3+v_4 \geqslant 7+6+6+0=19$，即 $v_1+v_2+v_3+v_4 \geqslant 19$。

综合情形 1 和情形 2 可知，引理 3 结论成立。证毕。

定理 1 对于图 3 所示的动态密码结构，若轮函数都是双射，则 $l(\forall l \geqslant 1)$ 轮差分特征中活动轮函数的个数 $\geqslant N(l)$，其中

$$N(l)=\begin{cases} l, & l=6t(t \geqslant 1) \text{或} 6t+1(t \geqslant 3) \\ l-1, & \text{其他} \end{cases}$$

证明 分 3 种情形进行讨论。

情形 1 $l=6t(t \geqslant 1)$。

由引理 2 的 1)可知，6 轮差分特征中活动轮函数的个数 $\geqslant 6$，因此 $6t$ 轮差分特征中活动轮函数的个数 $\geqslant 6t$，本情形下定理 1 结论成立。

情形 2 $l=6t+1(t \geqslant 3)$。

设图 3 所示的动态密码结构的 $6t+1$ 轮差分特征为

$$\Delta X^{(0)} \xrightarrow{6(v_1)} \Delta X^{(1)} \cdots \xrightarrow{6(v_t)} \Delta X^{(t)} \xrightarrow{1(v_{t+1})} \Delta X^{(t+1)} \quad (1 \leqslant \Delta X^{(i)} \leqslant 15, 0 \leqslant i \leqslant t+1)$$

其中，$\Delta X^{(i-1)} \xrightarrow{6(v_i)} \Delta X^{(i)} (1 \leqslant i \leqslant t)$ 表示第 $i(1 \leqslant i \leqslant t)$ 个 6 轮差分特征，$\Delta X^{(t)} \xrightarrow{1(v_{t+1})} \Delta X^{(t+1)}$ 表示最后一轮差分特征。由引理 2 的 1)可知 $v_i \geqslant 6(1 \leqslant i \leqslant t)$，由引理 3 可知 $v_{t-2}+v_{t-1}+v_t+v_{t+1} \geqslant 19$，因此 $v_1+v_2+\cdots+v_t+v_{t+1}=(v_1+v_2+\cdots+v_{t-3})+(v_{t-2}+v_{t-1}+v_t+v_{t+1}) \geqslant 6(t-3)+19=6t+1$，本情形下定理 1 结论成立。

情形 3 $l=6t+1(0 \leqslant t \leqslant 2)$ 或 $l=6t+m(t \geqslant 0, 2 \leqslant m \leqslant 5)$。

由引理 2 的 1)可知，6 轮差分特征中活动轮函数的个数 $\geqslant 6$，因此 $6t$ 轮差分特征中活动轮函数的个数 $\geqslant 6t$，从而 $6t+1$ 轮差分特征中活动轮函数的个数 $\geqslant 6t$。由引理 1 可知，对 CLEFIA 密码结构而言，m 轮差分特征中活动轮函数的个数 $\geqslant m-1$，因此 $6t+m(t \geqslant 0, 2 \leqslant m \leqslant 5)$ 轮差分特征中活动轮函数的个数 $\geqslant 6t+m-1$，本情形下定理结论成立。

综合情形 1、情形 2 和情形 3 可知，定理 1 结论成立。证毕。

由定理 1，可得定理 2。

定理 2 对于图 3 所示的动态密码结构，若轮函数都是双射且轮函数的最大差分概率为 $P_{\max}$，则 $l(\forall l \geqslant 1)$ 轮最大差分特征概率 $\leqslant [p_{\max}]^{N(l)}$。其中，$N(l)$ 的含义如定理 1 所示。

最后，将本文结果与文献[14]中的动态密码结构的相应结果进行比较，如表 1 所示。

表 1 本文结果与文献[14]中相应结果的比较

密码结构	l 轮差分特征至少有 l 个活动轮函数的情形	l 轮差分特征至少有 $l-1$ 个活动轮函数的情形	l 轮动态密码结构包含的密码结构个数
I 型类 CLEFIA 动态密码结构	$l=6t(t \geqslant 1)$	$l \neq 6t(t \geqslant 1)$	2^l
II 型类 CLEFIA 动态密码结构	$l=6t(t \geqslant 1)$，$l=6t+1(t \geqslant 3)$	$l=6t+2,6t+3,6t+4,6t+5(t \geqslant 0)$ l=1,7,13	$2^{\lceil l/2 \rceil}$
本文提出的动态密码结构	$l=6t(t \geqslant 1)$，$l=6t+1(t \geqslant 3)$	$l=6t+2,6t+3,6t+4,6t+5(t \geqslant 0)$ l=1,7,13	$2^{6\lceil l/6 \rceil}$

由表 1 可知，对于本文提出的动态密码结构，当迭代轮数 $l=6t(t\geqslant 1)$ 或 $l=6t+1(t\geqslant 3)$ 时，$l(l\geqslant 1)$ 轮差分特征至少有 l 个活动轮函数，当迭代轮数 l 取其他值时，$l(l\geqslant 1)$ 轮差分特征至少有 $l-1$ 个活动轮函数。与文献[14]中的 I 型类 CLEFIA 动态密码结构相比，$6t+1(t\geqslant 3)$ 轮差分特征的活动轮函数个数的下界增加了 1。与文献[14]中的 II 型类 CLEFIA 动态密码结构相比，本文提出的动态密码结构在迭代轮数相同的情况下具有相同的活动轮函数个数的下界。另外还可以看出，在迭代轮数相同的情况下，本文提出的动态密码结构所包含的密码结构个数比 I 型类 CLEFIA 动态密码结构的相应结果略少（即 $2^{6\lfloor l/6\rfloor}<2^{l}$，显然 $l=6t(t\geqslant 1)$ 时二者相等），比 II 型类 CLEFIA 动态密码结构的相应结果要多（即 $2^{6\lfloor l/6\rfloor}>2^{\lceil l/2\rceil}$）。这里，$\lfloor x\rfloor$ 表示不大于 x 的最大整数，$\lceil x\rceil$ 表示不小于 x 的最小整数。

本文的研究结果对分组密码算法的设计与分析具有重要的指导意义。根据定理 2 可知，如果知道轮函数的最大差分概率 $P_{\max}$，就能估计出任意轮最大差分特征概率的上界。当采用本文提出的动态密码结构设计分组密码算法时，其抵抗差分密码分析的能力就有了依据。例如，一个输入规模为 128 bit 的分组密码算法采用图 3 所示的动态密码结构，且轮函数 f_0 和 f_1（如图 1 和图 2 所示）都采用 SDS 结构（代替–扩散–代替结构）[22]。其中，SDS 结构中的 S 变换是 4 个 AES[23]S 盒的并置，D 变换是 4 阶 MDS 矩阵（显然其差分分支数[23]为 5）。因 S 盒的最大差分概率为 2^{-6} [23]，故轮函数的差分概率 $\leqslant (2^{-6})^4=2^{-24}$ [22]，从而 $l(\forall l\geqslant 1)$ 轮最大差分特征概率 $\leqslant 2^{-24\times N(l)}$。例如，$l=6$ 时，6 轮最大差分特征概率 $\leqslant 2^{-24\times 6}=2^{-144}$。

4　实验分析

本文通过 Python 编程对 CLEFIA 动态密码结构差分特征活动轮函数个数的下界进行验证（实验环境为 Windows 10，I7-5500U 2.4 GHz，8 GB RAM），并将结果与 I 型类 CLEFIA 动态密码结构和 II 型类 CLEFIA 动态密码结构差分特征活动轮函数个数的下界进行比较。表 2 给出了不同迭代轮数 3 种密码结构差分特征活动轮函数个数下界的对比。

在实验分析中，将活动轮函数个数的下界的求解问题转换为混合整数线性规划（MILP, mixed integer linear programming）[24]问题，利用 Gurobi 软件求解 MILP 问题得到活动轮函数个数的下界。但是在实际差分密码分析中，真实差分特征的活动轮函数个数往往大于 MILP 方法得到的理论估计，所以实际的下界大于或等于估计的下界。

对 $l(l\geqslant 1)$ 轮 CLEFIA 动态密码结构差分特征活动轮函数个数的下界进行求解，基本过程概括如下。

步骤 1　对于 l 轮 CLEFIA 动态密码结构，其线性变换 $\boldsymbol{P}$ 的选择有 $2^{6\lfloor l/6\rfloor}$ 种，并存储 $\boldsymbol{P}$ 的所有可能的组合。

步骤 2　任意选择一种 $\boldsymbol{P}$ 的组合，当轮数 $i \bmod 6\neq 0(1\leqslant i\leqslant l)$，对于 CLEFIA 密码结构进行建模；当轮数 $i \bmod 6=0(1\leqslant i\leqslant l)$，对于选定 $\boldsymbol{P}$ 的 CLEFIA 变形密码结构进行建模，利用 MILP 求解活动轮函数的个数并记录。

步骤 3　重复步骤 2，直至遍历所有 $\boldsymbol{P}$ 的组合。

步骤 4　输出 CLEFIA 动态密码结构差分特征活动轮函数个数的下界。

具体建模过程如下。对于密码结构中的异或操作，设其输入差分为 $(x_{\text{in0}},x_{\text{in1}})$，输出差分为 x_{out}，引入辅助变量 d，则上述变量的取值范围均为 $\{0,1\}$，可以得到

$$\begin{aligned}&x_{\text{in0}}+x_{\text{in1}}+x_{\text{out}}\geqslant 2d\\&d\geqslant x_{\text{in0}}\\&d\geqslant x_{\text{in1}}\\&d\geqslant x_{\text{out}}\end{aligned}$$

以第 $i(1\leqslant i\leqslant l, i \bmod 6\neq 0)$ 轮 CLEFIA 密码结构的建模为例，设输入差分为 $(x_{4i-4},x_{4i-3},x_{4i-2},x_{4i-1})$，输出差分为 $(x_{4i},x_{4i+1},x_{4i+2},x_{4i+3})$，$d_j,d_{j+1}$ 为引入的辅助变量，

表 2　**3 种密码结构差分特征活动轮函数个数下界的对比**

密码结构	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
I 型类 CLEFIA 动态密码结构	0	1	2	3	4	6	6	7	8	9	10	12	12	13	14	15	16	18	18	19
II 型类 CLEFIA 动态密码结构	0	1	2	3	4	6	6	7	8	9	10	12	12	13	14	15	16	18	19	19
本文提出的动态密码结构	0	1	2	3	4	6	6	7	8	9	10	12	12	13	14	15	16	18	19	19

可以构建

$$\begin{cases} x_{4i-4}+x_{4i-3}+x_{4i} \geqslant 2d_j \\ d_j \geqslant x_{4i-4} \\ d_j \geqslant x_{4i-3} \\ d_j \geqslant x_{4i} \end{cases}$$

$$\begin{cases} x_{4i-2}+x_{4i-1}+x_{4i+2} \geqslant 2d_{j+1} \\ d_{j+1} \geqslant x_{4i-2} \\ d_{j+1} \geqslant x_{4i-1} \\ d_{j+1} \geqslant x_{4i+2} \end{cases}$$

以第 $i(i=6t,t\geqslant 1)$ 轮 CLEFIA 动态密码结构的建模为例，当线性变换 $\boldsymbol{P}=\begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ 时，设输入差分为 $(x_{4i-4},x_{4i-3},x_{4i-2},x_{4i-1})$，输出差分为 $(x_{4i},x_{4i+1},x_{4i+2},x_{4i+3})$，$d_j,d_{j+1},d_{j+2}$ 为引入的辅助变量，可以构建

$$\begin{cases} x_{4i-4}+x_{4i-3}+x_{4i+2} \geqslant 2d_j \\ d_j \geqslant x_{4i-4} \\ d_j \geqslant x_{4i-3} \\ d_j \geqslant x_{4i+2} \end{cases}$$

$$\begin{cases} x_{4i-2}+x_{4i-1}+x_{4i} \geqslant 2d_{j+1} \\ d_{j+1} \geqslant x_{4i-2} \\ d_{j+1} \geqslant x_{4i-1} \\ d_{j+1} \geqslant x_{4i} \end{cases}$$

$$\begin{cases} x_{4i-4}+x_{4i-2}+x_{4i+3} \geqslant 2d_{j+2} \\ d_{j+2} \geqslant x_{4i-4} \\ d_{j+2} \geqslant x_{4i-2} \\ d_{j+2} \geqslant x_{4i+3} \end{cases}$$

对于每一轮的输入差分 $(x_{4i},x_{4i+1},x_{4i+2},x_{4i+3})$，活动轮函数的个数取决于输入差分的第一分支和第三分支，即 f_0 和 f_1 的输入差分，因此活动轮函数个数下界的求解可表示为 $\min\sum_{i=0}^{l-1}x_{4i}+x_{4i+2}$。利用 Gurobi 软件对该 MILP 问题进行求解即可得到 CLEFIA 动态密码结构差分特征活动轮函数个数的下界。

通过实验分析可得 1～20 轮 CLEFIA 动态密码结构差分特征活动轮函数个数的下界，并且实验结果与推导结果相同。

5 结束语

本文提出了一种动态密码结构，该动态密码结构的特点是第 $6t(\forall t\geqslant 1)$ 轮中的扩散层可以从 $\{0,1\}^4$ 上的多个线性双射（对应于 4 阶 0-1 可逆矩阵）中任意选取，即 $6t(\forall t\geqslant 1)$ 轮中的扩散层是动态可变的，因此该动态密码结构包含多个分组密码结构。本文通过对 6 轮差分特征的传递规律的分析，在轮函数都是双射的条件下，证明了 $l(l\geqslant 1)$ 轮差分特征中活动轮函数个数的下界为 $N(l)$，从而若设轮函数的最大差分概率为 $P_{\max}$，则 l 轮动态密码结构的最大差分特征概率 $\leqslant[p_{\max}]^{N(l)}$。对于本文提出的动态密码结构，还有一些问题需要进一步研究，例如，该动态密码结构抵抗不可能差分分析、零相关线性分析以及积分分析等分析方法的能力如何？同时，能否找到更合适的线性变换，使相同轮数的差分特征具有更多的活动轮函数，也值得进一步研究。

参考文献：

[1] 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.

[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 X Y, LIU T. The research of dynamic symmetric cipher algorithm[J]. Network Security Technology & Application, 2006(3): 69-71.

[3] 杨宏志. 对称密码算法簇设计及其仿真[D]. 郑州: 信息工程大学, 2010.
YANG H Z. Research on the design and simulation of symmetric cipher cluster[D]. Zhengzhou: Information Engineering University, 2010.

[4] 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 J Y, LIU T, HU X Y. Research and implementation of dynamic SMS4 algorithm[J]. Network Security Technology & Application, 2008(9): 92-93.

[5] ZHOU S Y, PENG M M, XIAO X H. An improvement of SMS4 algorithm based on dynamic[J]. Microelectronics & Computer, 2011, 28(9): 86-88.

[6] 周术洋. 基于动态思想的 SMS4 算法研究[D]. 长沙: 湖南大学, 2011.
ZHOU S Y. An improvement of SMS4 algorithm based on dynamic ideas[D]. Changsha: Hunan University, 2011.

[7] AGARWAL P, SINGH A, KILICMAN A. Development of key-dependent dynamic S-Boxes with dynamic irreducible polynomial

and affine constant[J]. Advances in Mechanical Engineering, 2018, 10(7): 1-18.

[8] 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 L K, ZHANG R T. Novel software block cipher using dynamic S-box and P-box[J]. Computer Science, 2009, 36(2): 78-81.

[9] ZHAO G S, WANG J. Security analysis and enhanced design of a dynamic block cipher[J]. China Communications, 2016, 13 (1): 150-160.

[10] IBRAHIM S, ABBAS A M. Efficient key-dependent dynamic S-boxes based on permutated elliptic curves[J]. Information Sciences, 2021, 558: 246-264.

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

[12] 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: 信息工程大学, 2016.
YIN J. Research on security of several types of block cipher structures against differential and linear analysis[D]. Zhengzhou: Information Engineering University, 2016.

[13] 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.

[14] 杨继林. 类 CLEFIA 动态密码结构抗差分和线性分析能力评估[D]. 郑州: 信息工程大学, 2019.
YANG J L. Evaluation of anti-differential and linear analysis ability of CLEFIA-like dynamic cipher structure[D]. Zhengzhou: Information Engineering University, 2019.

[15] 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.

[16] 王健康. 几类分组密码模型的安全性分析[D]. 郑州: 信息工程大学, 2013.
WANG J K. Security analysis of several block cipher models[D]. Zhengzhou: Information Engineering University, 2013.

[17] SHIRAI T, SHIBUTANI K. Improving immunity of feistel ciphers against differential cryptanalysis by using multiple MDS matrices[M]. Springer: Berlin, 2004.

[18] SHIRAI T, PRENEEL B. On feistel ciphers using optimal diffusion mappings across multiple rounds[C]//Advances in Cryptology - ASIACRYPT 2004. Berlin: Springer, 2004: 1-15.

[19] WANG Q J, BOGDANOV A. The provable constructive effect of diffusion switching mechanism in CLEFIA-type block ciphers[J]. Information Processing Letters, 2012, 112(11): 427-432.

[20] 金晨辉, 郑浩然, 张少武. 密码学[M]. 北京: 高等教育出版社, 2009.
JIN C H, ZHENG H R, ZHANG S W. Cryptography[M]. Beijing: Higher Education Press, 2009.

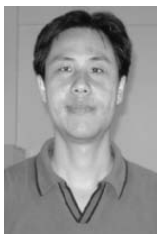
[21] SCHNEIER B, KELSEY J. Unbalanced feistel networks and block cipher design[C]//International Workshop on Fast Software Encryption. Berlin: Springer, 1996: 121-144.

[22] CHOY J, KHOO K. New applications of differential bounds of the SDS structure[C]// International Conference on Information Security. Berlin: Springer, 2008: 367-384.

[23] 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, 2000.
WU W L, FENG D G, ZHANG W T. Design and analysis of block cipher[M]. Beijing: Tsinghua University Press, 2000.

[24] MOUHA N, WANG Q J, GU D W, et al. Differential and linear cryptanalysis using mixed-integer linear programming[J]. Lecture Notes in Computer Science, 2012, 7357(5): 57-76.

[作者简介]



王念平（1972– ），男，河南洛宁人，博士，信息工程大学教授、博士生导师，主要研究方向为密码学、信息安全等。

郭祉成（1996– ），男，河南鹿邑人，信息工程大学硕士生，主要研究方向为分组密码设计与分析。