类 Piccolo 结构的差分安全性评估

王念平[1]，殷勍[2]
（1. 信息工程大学密码工程学院，河南 郑州 450004；2. 航天工程大学，北京 101416）

摘 要：为丰富分组密码的设计，提出类 Piccolo 结构及其设计原理，并深入研究了类 Piccolo 结构抵抗差分密码分析的能力。通过研究差分特征的输入输出传递特性，得到任意轮类 Piccolo 结构的活动轮函数个数的一个下界。分析结果表明，在轮函数都是双射的条件下，当迭代轮数 $l\geqslant 6$ 时，l 轮类 Piccolo 结构的活动轮函数个数$\geqslant l$；当迭代轮数 l 为 1,2,3,4,5 时，l 轮类 Piccolo 结构的活动轮函数个数$\geqslant l-1$。

关键词：类 Piccolo 结构；差分密码分析；活动轮函数
中图分类号：TN918.1
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2022037

Differential security evaluation of Piccolo-like structure

WANG Nianping[1], YIN Qing[2]
1. School of Crytography Engineering, Information Engineering University, Zhengzhou 450004, China
2. Space Engineering University, Beijing 101416, China

Abstract: In order to diversify the design of block cipher, Piccolo-like structure was proposed with principles of design. Security evaluation for Piccolo-like structure against differential cryptanalysis was deeply studied. By studying the input-output propagation characteristics of differential characteristics, the lower bound on the number of active round functions for arbitrary round Piccolo-like 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 Piccolo-like structure if $l\geqslant 6$, and there are at least $l-1$ active round functions for l-round Piccolo-like structure if l is 1,2,3,4,5.

Keywords: Piccolo-like structure, differential cryptanalysis, active round function

0 引言

分组密码作为现代密码学的重要组成部分，在信息安全领域有着广泛的应用。分组密码具有易于标准化、便于软硬件实现和容易同步等优点[1-2]，但也有一定的缺陷。例如，分组密码不能隐蔽数据模式，即相同的密文蕴含着相同的明文组，这是因为分组密码使用的是一个不随时间变化的固定变换。同时，分组密码不能抵抗组的重放、嵌入和删除等攻击。但上述的缺陷可以通过在加密过程中引入少量记忆加以克服，例如，可以通过密码分组链接（CBC, cipher block chaining）方式来克服[2-3]。另外，分组密码的安全性很难被证明。尽管“可证明安全性”的研究发展很快，但目前的分组密码大多是“看起来安全”的，还没有哪一个著名的分组密码真正被证明是安全的，至多证明了局部安全性。

对于分组密码，目前还存在一些问题值得考虑。一是分组密码算法的标准化。分组密码的大量社会化应用呼唤密码算法的标准化。二是分组密码设计和分析理论的研究。作为分组密码的研究者，总是希望从理论上解释一些设计方法的合理性，并将一些分析方法理论化，而不仅仅是停留在设计经验和直观分析的层次上。例如在一定假设条件下的

收稿日期：2021−11−29；**修回日期**：2022−01−18
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)

可证明安全性和伪随机性常常是研究者追求的一个目标。三是分组密码安全性分析的自动化。这是计算机技术与密码分析的有机结合。将一些密码分析方法程序化，往往可以提升分析的深度，弥补手工分析的不足。四是分组密码算法评估的实用化。算法的评估不仅要考虑在传统数学模型下的安全性，还应结合实现和应用环境评估算法的安全性，例如在侧信道模型下的安全性。本文的研究属于第二项内容。事实上，分组密码的整体结构对分组密码的安全性有很大影响。因此，研究分组密码结构的安全性一直是分组密码研究领域的重要内容。

差分密码分析[4]是一种典型的分组密码分析方法。差分密码分析能否成功主要取决于所利用的差分特征概率的大小。文献[5]指出，在最大差分特征概率足够小的情况下，就认为该密码算法对差分密码分析是免疫的。但在现实中，计算最大差分特征概率有一定的困难，且较难实现，所以就退而求其次——计算最大差分特征概率的上界，而最大差分特征概率的上界的计算取决于活动轮函数或活动 S 盒个数的下界。需要指出的是，在计算差分特征的活动轮函数或活动 S 盒个数的下界时，一般并不考虑轮函数和 S 盒的具体细化结构，而只是假设它们是双射的即可，从而所得的结果更具普遍性。文献[6-9]就是基于这样的思路进行分析的。

Piccolo 结构[10-11]是从 Piccolo 算法[12]中归结出来的一种密码结构，如图 1 所示。其设计特点在于块移位变换 RP 不直接对 4 个分块 Y_0、Y_1、Y_2、Y_3 进行移位，而是对平均分成的 8 个子分块进行移位。文献[10]研究了 Piccolo 结构抵抗差分密码分析的能力，证明了 $k(k\geqslant 1)$ 轮差分特征至少有 $k-1$ 个活动轮函数和 $(n+1)(k-1)$ 个活动 S 盒（$n+1$ 是轮函数中 P 变换的差分分支数）。文献[11]改进了文献[10]中的结果，证明了 $k(k\geqslant 6)$ 轮差分特征至少有 k 个活动轮函数和 $(n+1)k$ 个活动 S 盒，并指出活动轮函数个数的下界结果是不可改进的，所谓不可改进，是指确实存在一类差分特征，其活动轮函数的个数恰好达到了给出的下界。本文在此基础上，提出 32 种类 Piccolo 结构（包括文献[10-11]中的 Piccolo 结构），并对这些类 Piccolo 结构进行了差分密码分析，给出了活动轮函数和活动 S 盒个数的一个下界。

本文的结果与文献[10-11]相比，改进之处在于文献[10-11]只是针对 Piccolo 结构这一种密码结构进行分析的，而本文是针对提出的 32 种类 Piccolo 结构进行分析的。本文的结果比文献[10]中的结果要好，比文献[11]中的结果更具一般性。

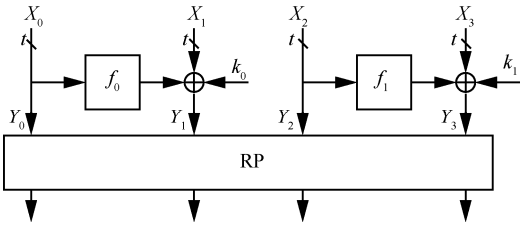


图 1 Piccolo 结构

1 预备知识

1.1 基本概念

定义 1[13] 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

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

其中，“$|\cdot|$”和“$\#\{\cdot\}$”表示集合的基数。

定义 2[1] $r(r\geqslant 1)$ 轮差分特征 Ω 是一个差分序列 $\alpha_0,\alpha_1,\cdots,\alpha_r$，其中 α_0 是明文对 Y_0 和 Y_0^* 的差分，$\alpha_i(1\leqslant i\leqslant r)$ 是第 i 轮输出 Y_i 和 Y_i^* 的差分。

定义 3[14] 输入差分非零的轮函数（S 盒），称为活动轮函数（S 盒）。

定义 4 $r(r\geqslant 1)$ 轮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。

本文称 $r(r\geqslant 1)$ 轮差分特征的活动指标为 $r(r\geqslant 1)$ 轮 Piccolo 结构的活动指标。本文中，将 n 元块移位变换 $\begin{pmatrix}0 & 1 & \cdots & n-1\\ i_0 & i_1 & \cdots & i_{n-1}\end{pmatrix}$ 简记为 $(i_0i_1\cdots i_{n-1})$，它表示按从左到右的顺序将原来第 i_j 个分块 a_{i_j} 移动到第 $j(j=0,1,\cdots,n-1)$ 个分块的位置，即 $(a_0,a_1,\cdots,a_{n-1})\to(a_{i_0},a_{i_1},\cdots,a_{i_{n-1}})$。

1.2 类 Piccolo 结构描述

图 2 是一轮类 Piccolo 结构，其中 $X_0,X_1,X_2,X_3\in Z_2^t$ 是输入，f_0,f_1 是轮函数，$k_0,k_1\in Z_2^t$ 是子密钥，块移位变换 $\sigma\in A$ 对 Y_0,Y_1,Y_2,Y_3 平均分成的 8 个子分块进行移位。其中，集合 A 由 32 个 8 元块移位变换构成，如表 1 所示。换句话说，类 Piccolo 结构就是以 $\sigma\in A$ 替换 Piccolo 结构[10-11]的块移位变换(27416305)所得到的结构。

显然，Piccolo 结构的块移位变换(27416305)也在集合 A 中，故 Piccolo 结构是类 Piccolo 结构的特例。

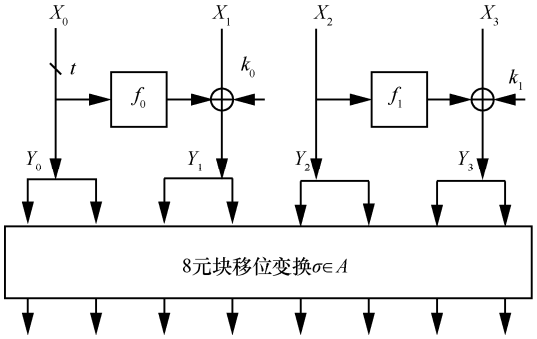


图 2　类 Piccolo 结构

表 1　　**集合 A**

变换 1~8	变换 9~16	变换 17~24	变换 25~32
(26043715)	(26513740)	(27043651)	(27513604)
(26057314)	(26417350)	(27056341)	(27416305)
(62503741)	(62143705)	(72503614)	(72143650)
(62407351)	(62157304)	(72406315)	(72156340)
(36402715)	(36152740)	(37402651)	(37152604)
(63052741)	(63412705)	(73052614)	(73412650)
(36507214)	(36147250)	(37506241)	(37146205)
(73046215)	(73516240)	(63047251)	(63517204)

表 1 中，8 元块移位变换 $(i_0 i_1 \cdots i_7)$ 表示移位变换 $\begin{pmatrix} 0 & 1 & \cdots & 7 \\ i_0 & i_1 & \cdots & i_7 \end{pmatrix}$（下同）。

1) 轮函数 f_0, f_1

如图 3 所示，轮函数 f_0, f_1 都采用 SPS 结构，这里 S 表示 n 个 $m\times m$ 双射 S 盒（n 为偶数且 $nm=t$，t 为输入块 $X_i(i=0,1,2,3)$ 的比特数），P 表示 $(Z_2^m)^n \to (Z_2^m)^n$ 的线性变换 $x \to \boldsymbol{M}x$，$\boldsymbol{M}$ 表示有限域 GF(2^m) 上的 n 阶 MDS 矩阵。易知，P 变换的分支数（包括差分分支数和线性分支数[13]）为 $(n+1)$，且轮函数 f_0, f_1 都是双射。

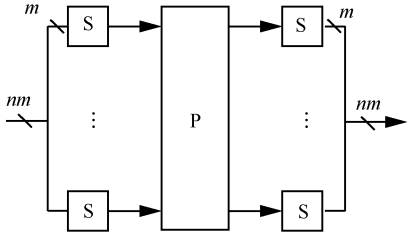


图 3　轮函数

2) 块移位变换 σ

集合 A 中的 8 元块移位变换 $\sigma=(i_0 i_1 \cdots i_7)$ 是满足以下 2 个条件的置换。

条件 1　$i_j \in \{2,3,6,7\}, j=0,1,4,5$；$i_k \in \{0,1,4,5\}, k=2,3,6,7$。

形象地说，满足条件 1 的 σ 如图 4 所示，即 $i_j(j=0,1,4,5)$ 只能从 $\{2,3,6,7\}$ 中选取，$i_k(k=2,3,6,7)$ 只能从 $\{0,1,4,5\}$ 中选取。

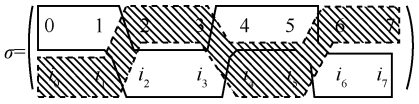


图 4　满足条件 1 的 σ

条件 2　$2i \in \{i_{2j}, i_{2j+1}\}, 2i+1 \in \{i_{2k}, i_{2k+1}\}$，$\forall i,j,k, 0 \leqslant i,j,k \leqslant 3, j \neq k$。

形象地说，满足条件 2 的 σ 如图 5 所示，即将每个大块 $2i$　$2i+1$ 中的 2 个小块 $2i$ 和 $2i+1$ 分别移位到不同的大块中去。

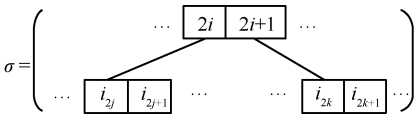


图 5　满足条件 2 的 σ

条件 1 和条件 2 共同保证了类 Piccolo 结构的扩散效果。

备注 1　为了叙述方便，将块移位变换是 σ 的类 Piccolo 结构称为 σ-Piccolo 结构。

性质 1[10]　设 $\boldsymbol{\alpha} \to \boldsymbol{\gamma} \to \boldsymbol{\delta} \to \boldsymbol{\beta}$ 是类 Piccolo 结构的轮函数 $f_j(j=0,1)$ 的差分对应，$\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$、$\gamma_0, \gamma_1, \cdots, \gamma_{n-1}$、$\delta_0, \delta_1, \cdots, \delta_{n-1}$ 和 $\beta_0, \beta_1, \cdots, \beta_{n-1}$ 依次为 $\boldsymbol{\alpha}$、$\boldsymbol{\gamma}$、$\boldsymbol{\delta}$ 和 $\boldsymbol{\beta}$ 的 n 个分块，且 $\alpha_j \to \gamma_j$ 或 $\delta_j \to \beta_j$ $(\forall j, 0 \leqslant j \leqslant n-1)$ 是 S 变换的第 j 个 S 盒的差分对应，$(\gamma_0, \gamma_1, \cdots, \gamma_{n-1}) \to (\delta_0, \delta_1, \cdots, \delta_{n-1})$ 是 P 变换的差分对应。$\forall \boldsymbol{\alpha} = (\alpha_0, \alpha_1, \cdots, \alpha_{n-1}) \in (Z_2^m)^n$，将 $\boldsymbol{\alpha}$ 看成 $Z_2^{\frac{mn}{2}}$ 上的 2 维列向量，即 $\boldsymbol{\alpha} = (\alpha_0, \alpha_1) \in (Z_2^{\frac{mn}{2}})^2$，并将 α_0, α_1 中非零元的个数记为 $W(\boldsymbol{\alpha})$，则对 $f_j : (Z_2^{\frac{mn}{2}})^2 \to (Z_2^{\frac{mn}{2}})^2$ 的差分对应 $\boldsymbol{\alpha} \to \boldsymbol{\beta}$，有 $\min\limits_{0 \neq a \in (Z_2^{\frac{mn}{2}})^2} \{W(\boldsymbol{\alpha}) + W(\boldsymbol{\beta})\} = 3$。

2　类 Piccolo 结构的活动轮函数和活动 S 盒个数的下界

为了分析方便，将 $X_i(i=0,1,2,3)$ 看成由左右规模相等的两部分 x_{2i} 和 x_{2i+1} 连接而成，即

$X_0 = x_0 \| x_1, X_1 = x_2 \| x_3, X_2 = x_4 \| x_5, X_3 = x_6 \| x_7$，其中“||”表示比特块的连接。那么，类 Piccolo 结构的输入就可表示为 $(x_0 \| x_1, x_2 \| x_3,\ x_4 \| x_5,\ x_6 \| x_7) \in (Z_2^{\frac{t}{2}})^8$，一轮类 Piccolo 结构（略去子密钥）的输入和输出关系式就可表示为

$$\begin{aligned}&Q_\sigma(x_0 \| x_1, x_2 \| x_3, x_4 \| x_5, x_6 \| x_7) = \\ &\sigma(x_0 \| x_1, f_0(x_0 \| x_1) \oplus \\ &x_2 \| x_3, x_4 \| x_5, f_1(x_4 \| x_5) \oplus x_6 \| x_7)\end{aligned}$$

首先，给出σ-Piccolo 结构的差分对应的结构形式。

定理 1 对任一σ-Piccolo 结构，设具有非零概率的一轮差分对应都具有如下形式

$$\begin{aligned}&(\alpha_0^{(0)} \| \alpha_1^{(0)}, \alpha_2^{(0)} \| \alpha_3^{(0)}, \alpha_4^{(0)} \| \alpha_5^{(0)}, \alpha_6^{(0)} \| \alpha_7^{(0)}) \to \\ &(\alpha_0^{(1)} \| \alpha_1^{(1)}, \alpha_2^{(1)} \| \alpha_3^{(1)}, \alpha_4^{(1)} \| \alpha_5^{(1)}, \alpha_6^{(1)} \| \alpha_7^{(1)})\end{aligned}$$

且记 $\alpha^{(k)} = (\alpha_0^{(k)} \| \alpha_1^{(k)}, \alpha_2^{(k)} \| \alpha_3^{(k)}, \alpha_4^{(k)} \| \alpha_5^{(k)}, \alpha_6^{(k)} \| \alpha_7^{(k)}), k = 0,1$，则相应轮函数 f_0 和 f_1 的差分对应分别为

$$f_0 : \alpha_0^{(0)} \| \alpha_1^{(0)} \to (\alpha_2^{(0)} \| \alpha_3^{(0)}) \oplus (\sigma_2^{-1}(\alpha^{(1)}) \| \sigma_3^{-1}(\alpha^{(1)}))$$

$$f_1 : \alpha_4^{(0)} \| \alpha_5^{(0)} \to (\alpha_6^{(0)} \| \alpha_7^{(0)}) \oplus (\sigma_6^{-1}(\alpha^{(1)}) \| \sigma_7^{-1}(\alpha^{(1)}))$$

并有

$$\begin{aligned}&p_{Q_\sigma}(\alpha_0^{(0)} \| \alpha_1^{(0)}, \alpha_2^{(0)} \| \alpha_3^{(0)}, \alpha_4^{(0)} \| \alpha_5^{(0)}, \alpha_6^{(0)} \| \alpha_7^{(0)}) \to \\ &(\alpha_0^{(1)} \| \alpha_1^{(1)}, \alpha_2^{(1)} \| \alpha_3^{(1)}, \alpha_4^{(1)} \| \alpha_5^{(1)}, \alpha_6^{(1)} \| \alpha_7^{(1)}) = \\ &p_{f_0}(\alpha_0^{(0)} \| \alpha_1^{(0)} \to (\alpha_2^{(0)} \| \alpha_3^{(0)}) \oplus (\sigma_2^{-1}(\alpha^{(1)}) \| \sigma_3^{-1}(\alpha^{(1)}))) \cdot \\ &p_{f_1}(\alpha_4^{(0)} \| \alpha_5^{(0)} \to (\alpha_6^{(0)} \| \alpha_7^{(0)}) \oplus (\sigma_6^{-1}(\alpha^{(1)}) \| \sigma_7^{-1}(\alpha^{(1)})))\end{aligned}$$

证明 $\forall \alpha^{(0)} \in (Z_2^{\frac{t}{2}})^8$，令 $f_0(x_0 \| x_1) = y_0 \| y_1$，$f_0(x_4 \| x_5) = y_4 \| y_5$，$f_0((x_0 \oplus \alpha_0^{(0)}) \| (x_1 \oplus \alpha_1^{(0)})) = y_0' \| y_1'$，$f_0((x_4 \oplus \alpha_4^{(0)}) \| (x_5 \oplus \alpha_5^{(0)})) = y_4' \| y_5'$，且令 $y_0 \oplus y_0' = \beta_0$，$y_1 \oplus y_1' = \beta_1$，$y_4 \oplus y_4' = \beta_4$，$y_5 \oplus y_5' = \beta_5$，则

$$\begin{aligned}&Q_\sigma(x_0 \| x_1, x_2 \| x_3, x_4 \| x_5, x_6 \| x_7) \oplus \\ &Q_\sigma((x_0 \| x_1) \oplus (\alpha_0^{(0)} \| \alpha_1^{(0)}), (x_2 \| x_3) \oplus \\ &(\alpha_2^{(0)} \| \alpha_3^{(0)}), (x_4 \| x_5) \oplus (\alpha_4^{(0)} \| \alpha_5^{(0)}), \\ &(x_6 \| x_7) \oplus (\alpha_6^{(0)} \| \alpha_7^{(0)})) = \\ &Q_\sigma(x_0 \| x_1, x_2 \| x_3, x_4 \| x_5, x_6 \| x_7) \oplus \\ &Q_\sigma((x_0 \oplus \alpha_0^{(0)}) \| (x_1 \oplus \alpha_1^{(0)}), \\ &(x_2 \oplus \alpha_2^{(0)}) \| (x_3 \oplus \alpha_3^{(0)}), (x_4 \oplus \alpha_4^{(0)}) \| \\ &(x_5 \oplus \alpha_5^{(0)}), (x_6 \oplus \alpha_6^{(0)}) \| (x_7 \oplus \alpha_7^{(0)})) = \\ &\sigma(x_0 \| x_1, x_2 \oplus y_0 \| x_3 \oplus y_1, x_4 \| \\ &x_5, x_6 \oplus y_4 \| x_7 \oplus y_5) \oplus \\ &\sigma((x_0 \oplus \alpha_0^{(0)}) \| (x_1 \oplus \alpha_1^{(0)}), \\ &(x_2 \oplus \alpha_2^{(0)} \oplus y_0') \| (x_3 \oplus \alpha_3^{(0)} \oplus y_1'), \\ &(x_4 \oplus \alpha_4^{(0)}) \| (x_5 \oplus \alpha_5^{(0)}), \\ &(x_6 \oplus \alpha_6^{(0)} \oplus y_4') \| (x_7 \oplus \alpha_7^{(0)} \oplus y_5')) = \\ &\sigma(\alpha_0^{(0)} \| \alpha_1^{(0)}, (\alpha_2^{(0)} \oplus \beta_0) \| (\alpha_3^{(0)} \oplus \beta_1), \\ &\alpha_4^{(0)} \| \alpha_5^{(0)}, (\alpha_6^{(0)} \oplus \beta_4) \| (\alpha_7^{(0)} \oplus \beta_5))\end{aligned}$$

记 $\alpha^{(1)} = \sigma(\alpha_0^{(0)} \| \alpha_1^{(0)}, (\alpha_2^{(0)} \oplus \beta_0) \| (\alpha_3^{(0)} \oplus \beta_1), \alpha_4^{(0)} \| \alpha_5^{(0)}, (\alpha_6^{(0)} \oplus \beta_4) \| (\alpha_7^{(0)} \oplus \beta_5))$，则

$$\begin{aligned}&\sigma^{-1}(\alpha^{(1)}) = (\alpha_0^{(0)} \| \alpha_1^{(0)}, (\alpha_2^{(0)} \oplus \beta_0) \| (\alpha_3^{(0)} \oplus \beta_1), \alpha_4^{(0)} \| \\ &\alpha_5^{(0)}, (\alpha_6^{(0)} \oplus \beta_4) \| (\alpha_7^{(0)} \oplus \beta_5))\end{aligned}$$

故 $(\alpha_2^{(0)} \| \alpha_3^{(0)}) \oplus (\sigma_2^{-1}(\alpha^{(1)}) \| \sigma_3^{-1}(\alpha^{(1)})) = \beta_0 \| \beta_1$，$(\alpha_6^{(0)} \| \alpha_7^{(0)}) \oplus (\sigma_6^{-1}(\alpha^{(1)}) \| \sigma_7^{-1}(\alpha^{(1)})) = \beta_4 \| \beta_5$。所以，轮函数 f_0 和 f_1 的差分对应分别为

$$f_0 : \alpha_0^{(0)} \| \alpha_1^{(0)} \to (\alpha_2^{(0)} \| \alpha_3^{(0)}) \oplus (\sigma_2^{-1}(\alpha^{(1)}) \| \sigma_3^{-1}(\alpha^{(1)}))$$

$$f_1 : \alpha_4^{(0)} \| \alpha_5^{(0)} \to (\alpha_6^{(0)} \| \alpha_7^{(0)}) \oplus (\sigma_6^{-1}(\alpha^{(1)}) \| \sigma_7^{-1}(\alpha^{(1)}))$$

易知

$$\begin{aligned}&Q_\sigma(x_0 \| x_1, x_2 \| x_3, x_4 \| x_5, x_6 \| x_7) \oplus \\ &Q_\sigma((x_0 \| x_1) \oplus (\alpha_0^{(0)} \| \alpha_1^{(0)}), (x_2 \| x_3) \oplus (\alpha_2^{(0)} \| \alpha_3^{(0)}), \\ &(x_4 \| x_5) \oplus (\alpha_4^{(0)} \| \alpha_5^{(0)}), (x_6 \| x_7) \oplus (\alpha_6^{(0)} \| \alpha_7^{(0)})) = \\ &(\alpha_0^{(1)} \| \alpha_1^{(1)}, \alpha_2^{(1)} \| \alpha_3^{(1)}, \alpha_4^{(1)} \| \alpha_5^{(1)}, \alpha_6^{(1)} \| \alpha_7^{(1)})\end{aligned}$$

成立，等价于

$$\begin{aligned}&(y_0 \oplus y_0') \| (y_1 \oplus y_1') = (\alpha_2^{(0)} \| \alpha_3^{(0)}) \oplus \\ &(\sigma_2^{-1}(\alpha^{(1)}) \| \sigma_3^{-1}(\alpha^{(1)}))\end{aligned}$$

和

$$\begin{aligned}&(y_4 \oplus y_4') \| (y_5 \oplus y_5') = (\alpha_6^{(0)} \| \alpha_7^{(0)}) \oplus \\ &(\sigma_6^{-1}(\alpha^{(1)}) \| \sigma_7^{-1}(\alpha^{(1)}))\end{aligned}$$

同时成立，故

$$\begin{aligned}&p_{Q_\sigma}(\alpha_0^{(0)} \| \alpha_1^{(0)}, \alpha_2^{(0)} \| \alpha_3^{(0)}, \alpha_4^{(0)} \| \alpha_5^{(0)}, \alpha_6^{(0)} \| \alpha_7^{(0)}) \to \\ &(\alpha_0^{(1)} \| \alpha_1^{(1)}, \alpha_2^{(1)} \| \alpha_3^{(1)}, \alpha_4^{(1)} \| \alpha_5^{(1)}, \alpha_6^{(1)} \| \alpha_7^{(1)}) = \\ &p_{f_0}(\alpha_0^{(0)} \| \alpha_1^{(0)} \to (\alpha_2^{(0)} \| \alpha_3^{(0)}) \oplus (\sigma_2^{-1}(\alpha^{(1)}) \| \sigma_3^{-1}(\alpha^{(1)}))) \cdot \\ &p_{f_1}(\alpha_4^{(0)} \| \alpha_5^{(0)} \to (\alpha_6^{(0)} \| \alpha_7^{(0)}) \oplus (\sigma_6^{-1}(\alpha^{(1)}) \| \sigma_7^{-1}(\alpha^{(1)})))\end{aligned}$$

证毕。

由定理 1，可得以下事实。

备注 2　对任一σ-Piccolo 结构，$k(k\geqslant 1)$轮差分特征$(\alpha_0^{(0)}\|\alpha_1^{(0)},\alpha_2^{(0)}\|\alpha_3^{(0)},\alpha_4^{(0)}\|\alpha_5^{(0)},\alpha_6^{(0)}\|\alpha_7^{(0)})\to(\alpha_0^{(1)}\|\alpha_1^{(1)},\alpha_2^{(1)}\|\alpha_3^{(1)},\alpha_4^{(1)}\|\alpha_5^{(1)},\alpha_6^{(1)}\|\alpha_7^{(1)})\to\cdots\to(\alpha_0^{(k)}\|\alpha_1^{(k)},\alpha_2^{(k)}\|\alpha_3^{(k)},\alpha_4^{(k)}\|\alpha_5^{(k)},\alpha_6^{(k)}\|\alpha_7^{(k)})$的活动指标就是集合$\{\alpha_i^{(j)}\|\alpha_{i+1}^{(j)}\,|\,i=0,4;\ 0\leqslant j\leqslant k-1\}$中非零元的个数。显然，活动指标与最后一轮输出差分$(\alpha_0^{(k)}\|\alpha_1^{(k)},\alpha_2^{(k)}\|\alpha_3^{(k)},\alpha_4^{(k)}\|\alpha_5^{(k)},\alpha_6^{(k)}\|\alpha_7^{(k)})$无关。

引理 1　对任一σ-Piccolo 结构，设$(\alpha_0^{(0)}\|\alpha_1^{(0)},\alpha_2^{(0)}\|\alpha_3^{(0)},\alpha_4^{(0)}\|\alpha_5^{(0)},\alpha_6^{(0)}\|\alpha_7^{(0)})\to(\alpha_0^{(1)}\|\alpha_1^{(1)},\alpha_2^{(1)}\|\alpha_3^{(1)},\alpha_4^{(1)}\|\alpha_5^{(1)},\alpha_6^{(1)}\|\alpha_7^{(1)})$是一轮差分对应，则$\alpha_2^{(0)}\|\alpha_3^{(0)},\alpha_6^{(0)}\|\alpha_7^{(0)},\alpha_0^{(1)}\|\alpha_1^{(1)},\alpha_4^{(1)}\|\alpha_5^{(1)}$不可能全为零，换句话说，具有非零概率的一轮差分对应不可能具有如下形式

$$(\alpha_0^{(0)}\|\alpha_1^{(0)},0\|0,\alpha_4^{(0)}\|\alpha_5^{(0)},0\|0)\to(0\|0,\alpha_2^{(1)}\|\alpha_3^{(1)},0\|0,\alpha_6^{(1)}\|\alpha_7^{(1)})$$

其中，$\alpha_0^{(0)}\|\alpha_1^{(0)}$和$\alpha_4^{(0)}\|\alpha_5^{(0)}$不全为零。

证明　（反证法）假设$\alpha_2^{(0)}\|\alpha_3^{(0)}=\alpha_6^{(0)}\|\alpha_7^{(0)}=\alpha_0^{(1)}\|\alpha_1^{(1)}=\alpha_4^{(1)}\|\alpha_5^{(1)}=0\|0$。因为$\sigma$满足条件 1，故由$\alpha_0^{(1)}\|\alpha_1^{(1)}=\alpha_4^{(1)}\|\alpha_5^{(1)}=0\|0$知$\sigma_2^{-1}(\alpha^{(1)})\|\sigma_3^{-1}(\alpha^{(1)})=\sigma_6^{-1}(\alpha^{(1)})\|\sigma_7^{-1}(\alpha^{(1)})=0\|0$，从而$(\alpha_2^{(0)}\|\alpha_3^{(0)})\oplus(\sigma_2^{-1}(\alpha^{(1)})\|\sigma_3^{-1}(\alpha^{(1)}))=(\alpha_6^{(0)}\|\alpha_7^{(0)})\oplus(\sigma_6^{-1}(\alpha^{(1)})\|\sigma_7^{-1}(\alpha^{(1)}))=0\|0$，再由定理 1 知，轮函数$f_0$和$f_1$的差分对应分别为$f_0:\alpha_0^{(0)}\|\alpha_1^{(0)}\to 0\|0$和$f_1:\alpha_4^{(0)}\|\alpha_5^{(0)}\to 0\|0$，而$\alpha_0^{(0)}\|\alpha_1^{(0)}$和$\alpha_4^{(0)}\|\alpha_5^{(0)}$不全为零，这与“轮函数都是双射”矛盾，故$\alpha_2^{(0)}\|\alpha_3^{(0)},\alpha_6^{(0)}\|\alpha_7^{(0)},\ \alpha_0^{(1)}\|\alpha_1^{(1)},\alpha_4^{(1)}\|\alpha_5^{(1)}$不可能全为零，引理 1 成立。证毕。

引理 2　对于任一σ-Piccolo 结构，以下 3 个结论成立。

结论 1　一轮 Piccolo 结构的活动指标大于或等于 0。

结论 2　2 轮 Piccolo 结构的活动指标大于或等于 1。

结论 3　3 轮 Piccolo 结构的活动指标大于或等于 2。

证明　1) 结论 1 显然成立，只证结论 2 和结论 3。

由备注 2 知，活动指标与最后一轮输出差分无关，从而为书写方便，有时将差分特征的最后一轮输出差分记为$(*\|*,*\|*,*\|*,*\|*)$。

2) 由定理 1，设σ-Piccolo 结构的 2 轮差分特征为

$$(\alpha_0^{(0)}\|\alpha_1^{(0)},\alpha_2^{(0)}\|\alpha_3^{(0)},\alpha_4^{(0)}\|\alpha_5^{(0)},\alpha_6^{(0)}\|\alpha_7^{(0)})\to(\alpha_0^{(1)}\|\alpha_1^{(1)},\alpha_2^{(1)}\|\alpha_3^{(1)},\alpha_4^{(1)}\|\alpha_5^{(1)},\alpha_6^{(1)}\|\alpha_7^{(1)})\to(*\|*,*\|*,*\|*,*\|*)$$

且第一轮的轮函数$f_0^{(1)}$和$f_1^{(1)}$的差分对应分别为

$$f_0^{(1)}:\alpha_0^{(0)}\|\alpha_1^{(0)}\to(\alpha_2^{(0)}\|\alpha_3^{(0)})\oplus(\sigma_2^{-1}(\alpha^{(1)})\|\sigma_3^{-1}(\alpha^{(1)}))$$
$$f_1^{(1)}:\alpha_4^{(0)}\|\alpha_5^{(0)}\to(\alpha_6^{(0)}\|\alpha_7^{(0)})\oplus(\sigma_6^{-1}(\alpha^{(1)})\|\sigma_7^{-1}(\alpha^{(1)}))$$

（反证法）假设$\alpha_0^{(0)}\|\alpha_1^{(0)}=\alpha_4^{(0)}\|\alpha_5^{(0)}=\alpha_0^{(1)}\|\alpha_1^{(1)}=\alpha_4^{(1)}\|\alpha_5^{(1)}=0\|0$。由$\alpha_0^{(0)}\|\alpha_1^{(0)}=0\|0$和轮函数$f_0^{(1)}$的差分对应$f_0^{(1)}:\alpha_0^{(0)}\|\alpha_1^{(0)}\to(\alpha_2^{(0)}\|\alpha_3^{(0)})\oplus(\sigma_2^{-1}(\alpha^{(1)})\|\sigma_3^{-1}(\alpha^{(1)}))$知$(\alpha_2^{(0)}\|\alpha_3^{(0)})\oplus(\sigma_2^{-1}(\alpha^{(1)})\|\sigma_3^{-1}(\alpha^{(1)}))=0\|0$，由$\alpha_4^{(0)}\|\alpha_5^{(0)}=0\|0$和轮函数$f_1^{(1)}$的差分对应$f_1^{(1)}:\alpha_4^{(0)}\|\alpha_5^{(0)}\to(\alpha_6^{(0)}\|\alpha_7^{(0)})\oplus(\sigma_6^{-1}(\alpha^{(1)})\|\sigma_7^{-1}(\alpha^{(1)}))$知$(\alpha_6^{(0)}\|\alpha_7^{(0)})\oplus(\sigma_6^{-1}(\alpha^{(1)})\|\sigma_7^{-1}(\alpha^{(1)}))=0\|0$。因为$\sigma$满足条件 1，从而由$\alpha_0^{(1)}\|\alpha_1^{(1)}=\alpha_4^{(1)}\|\alpha_5^{(1)}=0\|0$知$\sigma_2^{-1}(\alpha^{(1)})\|\sigma_3^{-1}(\alpha^{(1)})=\sigma_6^{-1}(\alpha^{(1)})\|\sigma_7^{-1}(\alpha^{(1)})=0\|0$，而$\sigma_2^{-1}(\alpha^{(1)})\|\sigma_3^{-1}(\alpha^{(1)})=\alpha_2^{(0)}\|\alpha_3^{(0)},\sigma_6^{-1}(\alpha^{(1)})\|\sigma_7^{-1}(\alpha^{(1)})=\alpha_6^{(0)}\|\alpha_7^{(0)}$，故$\alpha_2^{(0)}\|\alpha_3^{(0)}=\alpha_6^{(0)}\|\alpha_7^{(0)}=0\|0$，即$\alpha_2^{(0)}=\alpha_3^{(0)}=\alpha_6^{(0)}=\alpha_7^{(0)}=0$。再由假设条件$\alpha_0^{(0)}\|\alpha_1^{(0)}=\alpha_4^{(0)}\|\alpha_5^{(0)}=0\|0$知$\alpha_0^{(0)}=\alpha_1^{(0)}=\alpha_4^{(0)}=\alpha_5^{(0)}=0$，于是$\alpha_2^{(0)}=\alpha_3^{(0)}=\alpha_6^{(0)}=\alpha_7^{(0)}=\alpha_0^{(0)}=\alpha_1^{(0)}=\alpha_4^{(0)}=\alpha_5^{(0)}=0$，即

$$(\alpha_0^{(0)}\|\alpha_1^{(0)},\alpha_2^{(0)}\|\alpha_3^{(0)},\alpha_4^{(0)}\|\alpha_5^{(0)},\alpha_6^{(0)}\|\alpha_7^{(0)})=(0\|0,0\|0,0\|0,0\|0)$$

这与“非平凡差分对应”的含义矛盾，故$\alpha_0^{(0)}\|\alpha_1^{(0)}$、$\alpha_4^{(0)}\|\alpha_5^{(0)}$、$\alpha_0^{(1)}\|\alpha_1^{(1)}$、$\alpha_4^{(1)}\|\alpha_5^{(1)}$不全为零，进而由备注 2 知，2 轮 Piccolo 结构的活动指标大于或等于1。

3) 由定理 1，设σ-Piccolo 结构的 3 轮差分特征为

$$(\alpha_0^{(0)}\|\alpha_1^{(0)},\alpha_2^{(0)}\|\alpha_3^{(0)},\alpha_4^{(0)}\|\alpha_5^{(0)},\alpha_6^{(0)}\|\alpha_7^{(0)})\to(\alpha_0^{(1)}\|\alpha_1^{(1)},\alpha_2^{(1)}\|\alpha_3^{(1)},\alpha_4^{(1)}\|\alpha_5^{(1)},\alpha_6^{(1)}\|\alpha_7^{(1)})\to(\alpha_0^{(2)}\|\alpha_1^{(2)},\alpha_2^{(2)}\|\alpha_3^{(2)},\alpha_4^{(2)}\|\alpha_5^{(2)},\alpha_6^{(2)}\|\alpha_7^{(2)})\to(*\|*,*\|*,*\|*,*\|*)$$

且第$i(i=1,2)$轮的轮函数的差分对应分别为

$$f_0^{(i)}:\alpha_0^{(i-1)}\|\alpha_1^{(i-1)}\to(\alpha_2^{(i-1)}\|\alpha_3^{(i-1)})\oplus(\sigma_2^{-1}(\alpha^{(i)})\|\sigma_3^{-1}(\alpha^{(i)}))$$
$$f_1^{(i)}:\alpha_4^{(i-1)}\|\alpha_5^{(i-1)}\to(\alpha_6^{(i-1)}\|\alpha_7^{(i-1)})\oplus(\sigma_6^{-1}(\alpha^{(i)})\|\sigma_7^{-1}(\alpha^{(i)}))$$

此时，$\alpha_0^{(0)}\|\alpha_1^{(0)}$、$\alpha_4^{(0)}\|\alpha_5^{(0)}$、$\alpha_0^{(2)}\|\alpha_1^{(2)}$和$\alpha_4^{(2)}\|\alpha_5^{(2)}$不可能全为零。否则，由

$\alpha_0^{(0)} \| \alpha_1^{(0)} = \alpha_4^{(0)} \| \alpha_5^{(0)} = 0 \| 0$ 知 $\alpha_0^{(0)} = \alpha_1^{(0)} = \alpha_4^{(0)} = \alpha_5^{(0)} = 0$，所以第一轮中 σ 的输入差分为 $(\alpha_0^{(0)} \| \alpha_1^{(0)}, * \| *, \alpha_4^{(0)} \| \alpha_5^{(0)}, * \| *) = (0 \| 0, * \| *, \ 0 \| 0, * \| *)$，记该输入差分为 $\alpha'^{(0)}$，则由 σ 满足条件 1 知，$\alpha_0^{(2)} = \sigma_0(\alpha'^{(0)}) = \alpha_1^{(2)} = \sigma_1(\alpha'^{(0)}) = \alpha_4^{(2)} \ = \sigma_4(\alpha'^{(0)}) = \alpha_5^{(2)} = \sigma_4(\alpha'^{(0)}) = 0$，故第 2 轮差分对应

$$(\alpha_0^{(1)} \| \alpha_1^{(1)}, \alpha_2^{(1)} \| \alpha_3^{(1)}, \alpha_4^{(1)} \| \alpha_5^{(1)}, \alpha_6^{(1)} \| \alpha_7^{(1)}) \to$$
$$(\alpha_0^{(2)} \| \alpha_1^{(2)}, \alpha_2^{(2)} \| \alpha_3^{(2)}, \alpha_4^{(2)} \| \alpha_5^{(2)}, \alpha_6^{(2)} \| \alpha_7^{(2)})$$

就变成

$$(\alpha_0^{(1)} \| \alpha_1^{(1)}, 0 \| 0, \alpha_4^{(1)} \| \alpha_5^{(1)}, 0 \| 0) \to$$
$$(0 \| 0, \alpha_2^{(2)} \| \alpha_3^{(2)}, 0 \| 0, \alpha_6^{(2)} \| \alpha_7^{(2)})$$

这与引理 1 矛盾，故 $\alpha_0^{(0)} \| \alpha_1^{(0)}$、$\alpha_4^{(0)} \| \alpha_5^{(0)}$、$\alpha_0^{(2)} \| \alpha_1^{(2)}$ 和 $\alpha_4^{(2)} \| \alpha_5^{(2)}$ 不可能全为零，以下分 2 种情形进行讨论。

情形 1　$\alpha_0^{(0)} \| \alpha_1^{(0)}$ 和 $\alpha_4^{(0)} \| \alpha_5^{(0)}$ 不全为零。

此时，一轮差分特征 $\to$ 的活动指标 $\geqslant 1$，再由结论 1 知，2 轮差分特征 $(\alpha_0^{(1)} \| \alpha_1^{(1)}, \alpha_2^{(1)} \| \alpha_3^{(1)}, \alpha_4^{(1)} \| \alpha_5^{(1)}, \alpha_6^{(1)} \| \alpha_7^{(1)}) \to (\alpha_0^{(2)} \| \alpha_1^{(2)}, \alpha_2^{(2)} \| \alpha_3^{(2)}, \alpha_4^{(2)} \| \alpha_5^{(2)}, \alpha_6^{(2)} \| \alpha_7^{(2)}) \to (* \| *, * \| *, * \| *, * \| *)$ 的活动指标大于或等于 1，从而 3 轮 Piccolo 结构的活动指标大于或等于 2。

情形 2　$\alpha_0^{(2)} \| \alpha_1^{(2)}$ 和 $\alpha_4^{(2)} \| \alpha_5^{(2)}$ 不全为零。

此时，一轮差分特征 $(\alpha_0^{(2)} \| \alpha_1^{(2)}, \alpha_2^{(2)} \| \alpha_3^{(2)}, \alpha_4^{(2)} \| \alpha_5^{(2)}, \alpha_6^{(2)} \| \alpha_7^{(2)}) \to (* \| *, * \| *, * \| *, * \| *)$ 的活动指标 $\geqslant 1$，再由结论 1 知，2 轮差分特征 $(\alpha_0^{(0)} \| \alpha_1^{(0)}, \alpha_2^{(0)} \| \alpha_3^{(0)}, \alpha_4^{(0)} \| \alpha_5^{(0)}, \alpha_6^{(0)} \| \alpha_7^{(0)}) \to (\alpha_0^{(1)} \| \alpha_1^{(1)}, \alpha_2^{(1)} \| \ \ \alpha_3^{(1)}, \alpha_4^{(1)} \| \alpha_5^{(1)}, \alpha_6^{(1)} \| \alpha_7^{(1)}) \to (* \| *, * \| *, * \| *, * \| *)$ 的活动指标大于或等于 1，从而 3 轮 Piccolo 结构的活动指标大于或等于 2。

综合情形 1 和情形 2，引理 2 成立。证毕。

接下来，设 $(\alpha_0 \| \alpha_1, \alpha_2 \| \alpha_3, \alpha_4 \| \alpha_5, \alpha_6 \| \alpha_7)$ 是 σ-Piccolo 结构的输入差分。若差分块 α_i 为非零差分块，则用“1”表示；若差分块 α_i 为零差分块，则用“0”表示，其中 $i = 0,1,2,\cdots,7$。那么，σ-Piccolo 结构的非零输入差分恰好有 $2^8-1=255$ 种表示，即 $\Delta_1 = (10000000)$，$\Delta_2 = (01000000)$，$\cdots$，$\Delta_{255} = (11111111)$（这种表示方法不妨称为“0”“1”表示）。易知，$f_0$ 为活动轮函数当且仅当左起第 1、2 位不全为零，f_1 为活动轮函数当且仅当左起第 5、6 位不全为零。

首先，给出输入输出差分块“0”“1”进行 XOR 运算需要满足的运算规则：设 $a,b,c,d \in \{0,1\}$ 分别是 $\alpha,\beta,\gamma,\delta \in Z_2^t$ 按照上述方法的“0”“1”表示，且设“$\wedge$”是按位与，“$\vee$”是按位或。

性质 2　差分经过 XOR 运算需要满足以下条件：设 $\alpha \oplus \beta = \gamma$，则

$$c = \begin{cases} a+b, & a \wedge b = 0 \\ 0 \text{或} 1, & a = b = 1 \end{cases}$$

性质 2 表示对于 $\alpha \oplus \beta = \gamma$，当 α,β 至少有一个为零时，有 $c = a+b$；当 α,β 都非零时，$\alpha \oplus \beta = \gamma$ 的值可能为零，也可能不为零，所以 $c = 0$ 或 1。

性质 3　差分经过轮函数需要满足以下条件：设 $f(\alpha \| \beta) = \gamma \| \delta$，则

$$a+b+c+d \begin{cases} \geqslant 3, & a \vee b = 1 \\ = 0, & a = b = 0 \end{cases}$$

性质 3 表示当轮函数的输入差分非零时，有 $a+b+c+d \geqslant 3$（因为输入差分和输出差分满足性质 1）；当轮函数的输入差分为零时，输出差分也为零。

根据性质 2 和性质 3，借助计算机，可以完成以下 3 个实验。

实验 1　计算机搜索 32 个 σ-Piccolo 结构，给出所有第一轮的活动指标为 0、第 2 轮的活动指标为 1、第 3 轮的活动指标为 1 的 3 轮差分特征的尾轮输出差分（二进制）。

实验 1 的具体结果如表 2 所示。通过表 2 发现，对于任一满足条件的 3 轮差分特征的尾轮输出差分 $\Delta = x_0x_1x_2x_3x_4x_5x_6x_7$，$x_0$ 和 x_1 至少有一个为“1”，$(\alpha_0^{(l)} \| \alpha_1^{(l)}, \alpha_2^{(l)} \| \alpha_3^{(l)}, \alpha_4^{(l)} \| \ \ \alpha_5^{(l)}, \alpha_6^{(l)} \| \alpha_7^{(l)})$ 和 x_5 至少有一个为“1”，故可得以下结论。

命题 1　对于任一 σ-Piccolo 结构，设 4 轮差分特征满足第一轮的活动指标为 0，第 2 轮的活动指标为 1，第 3 轮的活动指标为 1，则第 4 轮的活动指标必为 2。

引理 3　对于任一 σ-Piccolo 结构，当输入差分具有 $(0 \| 0, \alpha_2 \| \alpha_3, 0 \| 0, \alpha_6 \| \alpha_7)$ 形式时，以下 3 个结论至少有一个成立。

结论 1　前 2 轮 Piccolo 结构的活动指标大于或等于 2。

结论 2　前 3 轮 Piccolo 结构的活动指标大于或

表 2　　**实验 1 的具体结果**

块移位变换σ				满足条件的 3 轮差分特征的尾轮输出差分
(26417350)	(62143705)	(73052614)	(37506241)	(10001010)(10001110)(01000101)(01001101)(01100100)(11100100)(10011000)(11011000)
(26043715)	(62407351)	(37152604)	(73516240)	(10000110)(10001110)(01001001)(01001101)(01101000)(11101000)(10010100)(11010100)
(26513740)	(62157304)	(37402651)	(73046215)	(10000101)(10001101)(01001010)(01001110)(10100100)(11100100)(01011000)(11011000)
(27043651)	(72406315)	(36152740)	(63517204)	(10000110)(10001110)(01001001)(01001101)(10100100)(11100100)(01011000)(11011000)
(27513604)	(72156340)	(36402715)	(63047251)	(10000101)(10001101)(01001010)(01001110)(01101000)(11101000)(10010100)(11010100)
(26057314)	(62503741)	(73412650)	(37146205)	(10001001)(10001101)(01000110)(01001110)(10101000)(11101000)(01010100)(11010100)
(72143650)	(27416305)	(63052741)	(36507214)	(10001010)(10001110)(01000101)(01001101)(10101000)(11101000)(01010100)(11010100)
(27056341)	(72503614)	(63412705)	(36147250)	(10001001)(10001101)(01000110)(01001110)(01100100)(11100100)(10011000)(11011000)

等于 3。

结论 3　4 轮 Piccolo 结构的活动指标恰为 4。其中，$\alpha_2 \| \alpha_3, \alpha_6 \| \alpha_7$ 不全为零。

证明　只需证明结论 1 和结论 2 都不成立时，必有结论 3 成立即可。由引理 2 知，2 轮 Piccolo 结构的活动指标大于或等于 1，3 轮 Piccolo 结构的活动指标大于或等于 2，从而只需证明前 2 轮 Piccolo 结构的活动指标为 1，且前 3 轮 Piccolo 结构的活动指标为 2 时，必有结论 3 成立即可。

当输入差分具有 $(0\|0, \alpha_2^{(0)} \| \alpha_3^{(0)}, 0 \| 0, \alpha_6^{(0)} \| \alpha_7^{(0)})$ 形式时，要说明结论 3 成立，只需证明第一轮的活动指标为 0、第 2 轮的活动指标为 1、第 3 轮的活动指标为 1 的 4 轮差分特征恰有 4 个活动轮函数。由命题 1 知，这样的 4 轮差分特征中第 4 轮恰有 2 个活动轮函数，故 4 轮 Piccolo 结构的活动指标恰为 1+1+2=4，引理 3 成立。证毕。

定理 2　对于任一σ-Piccolo 结构，$k(k \geqslant 1)$ 轮 Piccolo 结构的活动指标大于或等于 $k-1$。

证明　（数学归纳法）当 $k = 1, 2, 3$ 时，由引理 2 知，定理 2 成立。

假设 $k < l (l \geqslant 4)$ 时定理 2 成立，以下证明 $k = l$ 时定理 2 成立。

对任一 l 轮差分特征 $(\alpha_0^{(0)} \| \alpha_1^{(0)}, \alpha_2^{(0)} \| \alpha_3^{(0)}, \alpha_4^{(0)} \| \alpha_5^{(0)}, \alpha_6^{(0)} \| \alpha_7^{(0)}) \rightarrow (\alpha_0^{(1)} \| \alpha_1^{(1)}, \alpha_2^{(1)} \| \alpha_3^{(1)}, \alpha_4^{(1)} \| \alpha_5^{(1)}, \alpha_6^{(1)} \| \alpha_7^{(1)}) \rightarrow \cdots \rightarrow (\alpha_0^{(l)} \| \alpha_1^{(l)}, \alpha_2^{(l)} \| \alpha_3^{(l)}, \alpha_4^{(l)} \| \alpha_5^{(l)}, \alpha_6^{(l)} \| \alpha_7^{(l)})$，分情况进行讨论。

情形 1　$\alpha_0^{(0)} \| \alpha_1^{(0)}, \alpha_4^{(0)} \| \alpha_5^{(0)}$ 不全为零。

此时，第一轮差分对应 $(\alpha_0^{(0)} \| \alpha_1^{(0)}, \alpha_2^{(0)} \| \alpha_3^{(0)}, \alpha_4^{(0)} \| \alpha_5^{(0)}, \alpha_6^{(0)} \| \alpha_7^{(0)}) \rightarrow (\alpha_0^{(1)} \| \alpha_1^{(1)}, \alpha_2^{(1)} \| \alpha_3^{(1)}, \alpha_4^{(1)} \| \alpha_5^{(1)}, \alpha_6^{(1)} \| \alpha_7^{(1)})$ 的活动指标大于或等于 1，由归纳假设，$l-1$ 轮差分特征 $(\alpha_0^{(1)} \| \alpha_1^{(1)}, \alpha_2^{(1)} \| \alpha_3^{(1)}, \alpha_4^{(1)} \| \alpha_5^{(1)}, \alpha_6^{(1)} \| \alpha_7^{(1)}) \rightarrow \cdots \rightarrow (\alpha_0^{(l)} \| \alpha_1^{(l)}, \alpha_2^{(l)} \| \alpha_3^{(l)}, \alpha_4^{(l)} \| \alpha_5^{(l)}, \alpha_6^{(l)} \| \alpha_7^{(l)})$ 的活动指标大于或等于 $l-2$，从而 l 轮 Piccolo 结构的活动指标大于或等于 $1+(l-2) = l-1$。

情形 2　$\alpha_0^{(0)} \| \alpha_1^{(0)}, \alpha_4^{(0)} \| \alpha_5^{(0)}$ 全为零。

此时，由引理 3，又可分为 3 种情形。

1) 前 2 轮差分特征 $(\alpha_0^{(0)} \| \alpha_1^{(0)}, \alpha_2^{(0)} \| \alpha_3^{(0)}, \alpha_4^{(0)} \| \alpha_5^{(0)}, \alpha_6^{(0)} \| \alpha_7^{(0)}) \rightarrow (\alpha_0^{(1)} \| \alpha_1^{(1)}, \alpha_2^{(1)} \| \alpha_3^{(1)}, \alpha_4^{(1)} \| \alpha_5^{(1)}, \alpha_6^{(1)} \| \alpha_7^{(1)}) \rightarrow (\alpha_0^{(2)} \| \alpha_1^{(2)}, \alpha_2^{(2)} \| \alpha_3^{(2)}, \alpha_4^{(2)} \| \alpha_5^{(2)}, \alpha_6^{(2)} \| \alpha_7^{(2)})$ 的活动指标大于或等于 2。

此时，由归纳假设，$l-2$ 轮差分特征 $(\alpha_0^{(2)} \| \alpha_1^{(2)}, \alpha_2^{(2)} \| \alpha_3^{(2)}, \alpha_4^{(2)} \| \alpha_5^{(2)}, \alpha_6^{(2)} \| \alpha_7^{(2)}) \rightarrow \cdots \rightarrow (\alpha_0^{(l)} \| \alpha_1^{(l)}, \alpha_2^{(l)} \| \alpha_3^{(l)}, \alpha_4^{(l)} \| \alpha_5^{(l)}, \alpha_6^{(l)} \| \alpha_7^{(l)})$ 的活动指标大于或等于 $l-3$，从而 l 轮 Piccolo 结构的活动指标大于或等于 $2+(l-3) = l-1$。

2) 前 3 轮差分特征 $(\alpha_0^{(0)} \| \alpha_1^{(0)}, \alpha_2^{(0)} \| \alpha_3^{(0)}, \alpha_4^{(0)} \| \alpha_5^{(0)}, \alpha_6^{(0)} \| \alpha_7^{(0)}) \rightarrow (\alpha_0^{(1)} \| \alpha_1^{(1)}, \alpha_2^{(1)} \| \alpha_3^{(1)}, \alpha_4^{(1)} \| \alpha_5^{(1)}, \alpha_6^{(1)} \| \alpha_7^{(1)}) \rightarrow (\alpha_0^{(2)} \| \alpha_1^{(2)}, \alpha_2^{(2)} \| \alpha_3^{(2)}, \alpha_4^{(2)} \| \alpha_5^{(2)}, \alpha_6^{(2)} \| \alpha_7^{(2)}) \rightarrow (\alpha_0^{(3)} \| \alpha_1^{(3)}, \alpha_2^{(3)} \| \alpha_3^{(3)}, \alpha_4^{(3)} \| \alpha_5^{(3)}, \alpha_6^{(3)} \| \alpha_7^{(3)})$ 的活动指标大于或等于 3。

此时，由归纳假设，$l-3$ 轮差分特征 $(\alpha_0^{(3)} \| \alpha_1^{(3)}, \alpha_2^{(3)} \| \alpha_3^{(3)}, \alpha_4^{(3)} \| \alpha_5^{(3)}, \alpha_6^{(3)} \| \alpha_7^{(3)}) \rightarrow \cdots \rightarrow (\alpha_0^{(l)} \| \alpha_1^{(l)}, \alpha_2^{(l)} \| \alpha_3^{(l)}, \alpha_4^{(l)} \| \alpha_5^{(l)}, \alpha_6^{(l)} \| \alpha_7^{(l)})$ 的活动指标大于或等于 $l-4$，从而 l 轮 Piccolo 结构的活动指标大于或等于 $3+(l-4) = l-1$。

3) 前 4 轮差分特征 $(\alpha_0^{(0)} \| \alpha_1^{(0)}, \alpha_2^{(0)} \| \alpha_3^{(0)}, \alpha_4^{(0)} \| \alpha_5^{(0)}, \alpha_6^{(0)} \| \alpha_7^{(0)}) \rightarrow (\alpha_0^{(1)} \| \alpha_1^{(1)}, \alpha_2^{(1)} \| \alpha_3^{(1)}, \alpha_4^{(1)} \| \alpha_5^{(1)}, \alpha_6^{(1)} \| \alpha_7^{(1)}) \rightarrow \cdots \rightarrow (\alpha_0^{(4)} \| \alpha_1^{(4)}, \alpha_2^{(4)} \| \alpha_3^{(4)}, \alpha_4^{(4)} \| \alpha_5^{(4)}, \alpha_6^{(4)} \| \alpha_7^{(4)})$ 的活动指标恰为 4。

此时，由归纳假设，$l-4$ 轮差分特征

$(\alpha_0^{(4)} \| \alpha_1^{(4)}, \alpha_2^{(4)} \| \alpha_3^{(4)},\ \alpha_4^{(4)} \| \alpha_5^{(4)},\ \alpha_6^{(4)} \| \alpha_7^{(4)}) \rightarrow \cdots \rightarrow (\alpha_0^{(l)} \| \alpha_1^{(l)}, \alpha_2^{(l)} \| \alpha_3^{(l)}, \alpha_4^{(l)} \| \alpha_5^{(l)}, \alpha_6^{(l)} \| \alpha_7^{(l)})$ 的活动指标 $\geqslant l-5$，从而 l 轮 Piccolo 结构的活动指标大于或等于 $4+(l-5)=l-1$。

综合情形 1 和情形 2，定理 2 成立。证毕。

实验 2 计算机搜索 32 个 σ-Piccolo 结构，给出 6 轮 Piccolo 结构的活动指标的最小值。

因篇幅所限，这里只以块移位变换 $\sigma=(72503614)$ 为例给出实验 2 的结果，具体如表 3 所示。其中第 x（十六进制）行第 y（十六进制）列交叉处的数值表示以 $(x\,y)$ 为首轮输入差分的 6 轮 Piccolo 结构的活动指标的最小值。例如，第 3 行第 e 列交叉处的数值为 6，就表示以 (3 e)=($\underline{1100}$ $\underline{0111}$) 为首轮输入差分的 6 轮 Piccolo 结构的活动指标的最小值为 6。这里，行数和列数都从 0 开始计算，$3=\underline{1100}=1\times2^0+1\times2^1+0\times2^2+0\times2^3$, $e=\underline{0111}=0\times 2^0+1\times 2^1+1\times2^2+1\times2^3$。另外，实验结果表明，使活动指标的最小值为 6 的 6 轮 Piccolo 结构的非零输入差分共有 67 个，使活动指标的最小值为 7 的 6 轮 Piccolo 结构的非零输入差分共有 164 个，使活动指标的最小值为 8 的 6 轮 Piccolo 结构的非零输入差分共有 24 个。

实验 2 结果表明，有以下结论成立。

命题 2 对于任一 σ-Piccolo 结构，6 轮 Piccolo 结构的活动指标大于或等于 6。

实验 3 对于任一 σ-Piccolo 结构，利用计算机筛选出活动指标为 6 的 6 轮差分特征的尾轮输出差分（十六进制），筛选出活动指标恰为 $k-1(k=1,2,3,4,5)$ 的 k 轮差分特征的首轮输入差分（十六进制）。

实验 3 的具体结果如表 4 所示。通过观察表 4 发现，对于任一 σ-Piccolo 结构，实验 3 中所求的尾轮输出差分和首轮输入差分没有重合，故可得以下结论。

命题 3 对于任一 σ-Piccolo 结构，若 6 轮 Piccolo 结构的活动指标为 6，则它的后面不可能“联接”活动指标为 $k-1(k=1,2,3,4,5)$ 的 k 轮差分特征。

引理 4 对于任一 σ-Piccolo 结构，设 $\alpha^{(0)} \rightarrow \alpha^{(1)} \rightarrow \cdots \rightarrow \alpha^{(6)} \rightarrow \cdots \rightarrow \alpha^{(6n-6)} \rightarrow \cdots \rightarrow \alpha^{(6n)}$ 为任一活动指标为 $6n$ 的 $6n$ 轮差分特征，则最后 6 轮差分特征 $\alpha^{(6n-6)} \rightarrow \cdots \rightarrow \alpha^{(6n)}$ 的活动指标必为 6。

证明 根据命题 2 可知，6 轮差分特征 $\alpha^{(6n-6)} \rightarrow \cdots \rightarrow \alpha^{(6n)}$ 的活动指标 $\geqslant 6$。若 $\alpha^{(6n-6)} \rightarrow \cdots \rightarrow \alpha^{(6n)}$ 的活动指标大于 6，则 $6(n-1)$ 轮差分特征 $\alpha^{(0)} \rightarrow \alpha^{(1)} \rightarrow \cdots \rightarrow \alpha^{(6)} \rightarrow \cdots \rightarrow \alpha^{(6n-6)}$ 的活动指标必小于 $6(n-1)$，这与命题 2 矛盾，故 $\alpha^{(6n-6)} \rightarrow \cdots \rightarrow \alpha^{(6n)}$ 的活动指标必为 6，引理 4 成立。

表 3 **实验 2 的结果**

输入差分	6 轮 Piccolo 结构的活动指标的最小值															
00~0f	—	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7
10~1f	7	8	8	7	7	8	8	7	7	8	7	7	7	8	7	7
20~2f	7	8	8	7	7	7	8	7	7	8	8	7	7	7	8	7
30~3f	7	7	7	7	6	7	7	7	6	7	7	7	7	6	6	7
40~4f	7	7	7	6	7	6	6	6	6	7	7	6	6	6	6	6
50~5f	7	8	7	7	6	8	7	7	7	7	7	7	7	6	7	7
60~6f	7	8	8	7	6	7	8	7	7	7	7	7	7	7	7	7
70~7f	7	7	7	7	6	7	7	7	6	7	7	7	6	6	6	7
80~8f	7	7	7	6	6	7	7	6	7	6	6	6	6	6	6	6
90~9f	7	8	8	7	7	7	7	7	6	8	7	7	7	7	7	7
a0~af	7	7	8	7	7	7	7	7	6	7	8	7	7	7	6	7
b0~bf	7	7	7	7	6	7	7	7	6	7	7	7	6	6	6	7
c0~cf	7	7	7	7	6	7	7	6	6	7	7	6	6	7	7	6
d0~df	7	8	7	6	6	6	7	6	6	7	7	6	7	6	7	6
e0~ef	7	7	8	6	6	7	7	6	6	7	6	6	7	7	6	6
f0~ff	7	7	7	7	6	7	7	7	6	7	7	7	6	6	6	7

表 4　　**实验 3 的具体结果**

块移位变换σ	活动指标为 6 的 6 轮差分特征的尾轮输出差分																		活动指标为 k−1（k=1,2,3,4,5）的 k 轮差分特征的首轮输入差分									
(26043715)	3	13	16	17	1a	23	25	29	2b	30	31	32	33	35	3a	46	47		4	7	8	b	c	d	e	f	40	44
(62407351)	52	53	56	57	5b	61	64	65	67	6e	6f	71	74	75	76	77	7a		48	49	4c	4d	68	70	80	84	86	88
(37152604)	7b	7e	7f	89	8b	92	98	9a	9b	9d	9f	a1	a3	a7	a9	ab	b2		8c	8e	94	b0	c0	c4	c8	cc	d0	d4
(73516240)	b5	b7	b8	b9	ba	bb	bd	bf	d9	db	e6	e7	f6	f7	f9	fb			e0	e8	f0							
(26513740)	3	13	16	1a	1b	23	25	27	29	30	31	32	33	36	39	45	47		4	7	8	b	c	d	e	f	40	44
(62157304)	52	54	56	57	5d	5f	61	63	65	67	6b	72	74	75	76	77	79		48	4a	4c	4e	58	70	80	84	85	88
(37402651)	7b	7d	7f	8a	8b	92	93	97	9a	9b	a1	a8	a9	ab	ae	af	b1		8c	8d	a4	b0	c0	c4	c8	cc	d0	d8
(73046215)	b6	b7	b8	b9	ba	bb	be	bf	d5	d7	ea	eb	f5	f7	fa	fb			e0	e4	f0							
(27043651)	3	13	16	17	1a	23	25	29	2b	30	31	32	33	35	3a	49	4b		4	7	8	b	c	d	e	f	40	44
(72406315)	52	58	5a	5b	5d	5f	61	63	67	69	6b	72	75	77	78	79	7a		46	48	4c	4e	54	70	80	84	88	89
(36152740)	7b	7d	7f	86	87	92	93	96	97	9b	a1	a4	a5	a7	ae	af	b1		8c	8d	a8	b0	c0	c4	c8	cc	d0	d4
(63517204)	b4	b5	b6	b7	ba	bb	be	bf	d9	db	e6	e7	f6	f7	f9	fb			e0	e8	f0							
(27513604)	3	13	16	1a	1b	23	25	27	29	30	31	32	33	36	39	4a	4b		4	7	8	b	c	d	e	f	40	44
(72156340)	52	53	57	5a	5b	61	68	69	6b	6e	6f	71	76	77	78	79	7a		45	48	4c	4d	64	70	80	84	88	8a
(36402715)	7b	7e	7f	85	87	92	94	96	97	9d	9f	a1	a3	a5	a7	ab	b2		8c	8e	98	b0	c0	c4	c8	cc	d0	d8
(63047251)	b4	b5	b6	b7	b9	bb	bd	bf	d5	d7	ea	eb	f5	f7	fa	fb			e0	e4	f0							
(26057314)	3	13	15	19	1b	23	26	27	2a	30	31	32	33	35	3a	46	47		4	7	8	b	c	d	e	f	40	44
(62503741)	51	54	55	57	5e	5f	62	63	66	67	6b	71	74	75	76	77	7a		48	49	4c	4d	58	70	80	84	86	88
(73412650)	7b	7e	7f	89	8b	91	93	97	99	9b	a2	a8	aa	ab	ad	af	b2		b5	b7	b8	b9	ba	bb	bd	bf	d6	d7
(37146205)	b5	b7	b8	b9	ba	bb	bd	bf	d6	d7	e9	eb	f6	f7	f9	fb			e0	e4	f0							
(26417350)	3	13	15	17	19	23	26	2a	2b	30	31	32	33	36	39	45	47		4	7	8	b	c	d	e	f	40	44
(62143705)	51	53	55	57	5b	62	64	66	67	6d	6f	72	74	75	76	77	79		48	4a	4c	4e	68	70	80	84	85	88
(73052614)	7b	7d	7f	8a	8b	91	98	99	9b	9e	9f	a2	a3	a7	aa	ab	b1		8c	8d	94	b0	c0	c4	c8	cc	d0	d4
(37506241)	b6	b7	b8	b9	ba	bb	be	bf	da	db	e5	e7	f5	f7	fa	fb			e0	e8	f0							
(27056341)	3	13	15	19	1b	23	26	27	2a	30	31	32	33	35	3a	49	4b		4	7	8	b	c	d	e	f	40	44
(72503614)	51	53	57	59	5b	62	68	6a	6b	6d	6f	72	75	77	78	79	7a		46	48	4c	4e	64	70	80	84	88	89
(63412705)	7b	7d	7f	86	87	91	94	95	97	9e	9f	a2	a3	a6	a7	ab	b1		8c	8d	98	b0	c0	c4	c8	cc	d0	d8
(36147250)	b4	b5	b6	b7	ba	bb	be	bf	d6	d7	e9	eb	f6	f7	f9	fb			e0	e4	f0							
(27416305)	3	13	15	17	19	23	26	2a	2b	30	31	32	33	36	39	4a	4b		4	7	8	b	c	d	e	f	40	44
(72143650)	51	58	59	5b	5e	5f	62	63	67	6a	6b	71	76	77	78	79	7a		45	48	4c	4d	54	70	80	84	88	8a
(63052741)	7b	7e	7f	85	87	91	93	95	97	9b	a2	a4	a6	a7	ad	af	b2		8c	8e	a8	b0	c0	c4	c8	cc	d0	d4
(36507214)	b4	b5	b6	b7	b9	bb	bd	bf	da	db	e5	e7	f5	f7	fa	fb			e0	e8	f0							

证毕。

定理 3　对于任一σ-Piccolo 结构，以下 2 个结论成立。

结论 1　$k(1\leqslant k\leqslant 5)$轮 Piccolo 结构的活动指标大于或等于$k-1$。

结论 2　$k(k\geqslant 6)$轮 Piccolo 结构的活动指标大于或等于k。

证明　1) 结论 1 由定理 2 即可证明。

2) 当$k=6n(n\geqslant 1)$时，由命题 2 可知，结论 2 成立。当$k=6n+m(n\geqslant 1,1\leqslant m\leqslant 5)$时，分以下 2 种情形进行讨论。

情形 1　前$6n$轮 Piccolo 结构的活动指标大于或等于$6n+1$。

此时，由定理 2 可知，后 m 轮差分特征$\alpha^{(6n)}\to\cdots\to\alpha^{(6n+m)}$的活动指标大于或等于$m-1$，所以$6n+m$轮 Piccolo 结构的活动指标大于或等于

$(6n+1)+(m-1)=6n+m$。

情形 2 前 $6n$ 轮 Piccolo 结构的活动指标恰为 $6n$ 时。

此时，设 $\alpha^{(0)}\to\cdots\to\alpha^{(6n)}\to\cdots\to\alpha^{(6n+m)}$ 为任一 $6n+m$ 轮差分特征，且 $6n$ 轮差分特征 $\alpha^{(0)}\to\cdots\to\alpha^{(6n)}$ 的活动指标为 $6n$。由引理 4 知，$\alpha^{(6n-6)}\to\cdots\to\alpha^{(6n)}$ 的活动指标为 6，再由命题 3 和定理 2 可知，后 m 轮差分特征 $\alpha^{(6n)}\to\cdots\to\alpha^{(6n+m)}$ 的活动指标大于或等于 m，所以 $6n+m$ 轮 Piccolo 结构的活动指标大于或等于 $6n+m$。

综合情形 1 和情形 2，定理 3 成立。证毕。

由定理 3 可得以下推论（注意：轮函数中的 P 变换的差分分支数为 $n+1$）。

推论 1 对于任一 σ-Piccolo 结构，以下 2 个结论成立。

结论 1 $k(1\leqslant k\leqslant 5)$ 轮差分特征中活动 S 盒的个数大于或等于 $(n+1)(k-1)$。

结论 2 $k(k\geqslant 6)$ 轮差分特征中活动 S 盒的个数大于或等于 $(n+1)k$。

3 结束语

本文提出了类 Piccolo 结构，并通过对差分传递规律的分析，得到了多轮类 Piccolo 结构的活动轮函数和活动 S 盒个数的一个下界。利用这些结果，结合轮函数或 S 盒的最大差分概率，给出类 Piccolo 结构的最大差分特征概率的上界。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，但类 Piccolo 结构抵抗其他攻击的能力如何值得进一步研究。

参考文献：

[1] 吴文玲, 冯登国, 张文涛. 分组密码的设计与分析: 第 2 版[M]. 北京: 清华大学出版社, 2009.
WU W L, FENG D G, ZHANG W T. Design and analysis of block cipher [M]. 2nd ed. Beijing: Tsinghua University Press, 2009.

[2] 温凤桐, 吴文玲, 温巧燕. 改进的 CBC 模式及其安全性分析[J]. 通信学报, 2007, 28(3): 52-56.
WEN F T, WU W L, WEN Q Y. Improved CBC mode of operation and its security analysis[J]. Journal on Communications, 2007, 28(3): 52-56.

[3] 冯登国, 裴定一. 密码学导引[M]. 北京: 科学出版社, 1999.
FENG D G, PEI D Y. Introduction to cryptography[M]. Beijing: Science Press, 1999.

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

[5] KNUDSEN L R. Practically secure Feistel ciphers[C]//Proceedings of 1993 International Workshop on Fast Software Encryption. Berlin: Springer, 1993: 211-221.

[6] 吴文玲, 贺也平. 一类广义 Feistel 密码的安全性评估[J]. 电子与信息学报, 2002, 24(9): 1177-1184.
WU W L, HE Y P. Security evaluation for a class of generalized Feistel ciphers[J]. Journal of Electronics and Information Technology, 2002, 24(9): 1177-1184.

[7] WANG Q Y, ZHANG B, JIN C H. Practical security against differential and linear cryptanalysis for SMS4-like cipher[J]. Journal of Networks, 2013, 8(8): 1689-1693.

[8] 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.

[9] ZHAO G Y, CHENG L, LI C, et al. On the practical security bound of GF-NLFSR structure with SPN round function[C]//Proceedings of 2014 8th International Conference on Provable Security. Berlin: Springer, 2014: 40-54.

[10] 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 Q, WANG N P. Security evaluation for Piccolo structure against differential and linear cryptanalysis[J]. Journal of Shandong University (Natural Science), 2016, 51(3): 132-142.

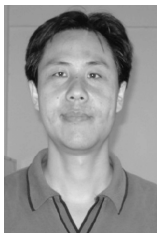
[11] 殷勍, 王念平. Piccolo 结构抵抗差分和线性密码分析能力的进一步评估[J]. 北京大学学报(自然科学版), 2018, 54(6): 1173-1178.
YIN Q, WANG N P. Further security evaluation for piccolo structure against differential and linear cryptanalysis[J]. Acta Scientiarum Naturalium Universitatis Pekinensis, 2018, 54(6): 1173-1178.

[12] SHIBUTANI K, ISOBE T, HIWATARI H, et al. Piccolo: an ultra-lightweight blockcipher[C]//Proceedings of 2011 International Conference on Cryptographic Hardware & Embedded Systems. Berlin: Springer, 2011: 342-357.

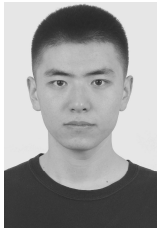
[13] 金晨辉, 郑浩然, 张少武. 密码学[M]. 北京: 高等教育出版社, 2009.
JIN C H, ZHENG H R, ZHANG S W. Cryptology[M]. Beijing: Higher Education Press, 2009.

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

[作者简介]



王念平（1973− ），男，河南洛阳人，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。



殷勍（1990− ），男，河南新乡人，航天工程大学助理工程师，主要研究方向为信息安全。