北京大学学报(自然科学版) 第 54 卷 第 6 期 2018 年 11 月
Acta Scientiarum Naturalium Universitatis Pekinensis, Vol. 54, No. 6 (Nov. 2018)
doi: 10.13209/j.0479-8023.2018.086

Piccolo 结构抵抗差分和线性密码分析能力的进一步评估

殷勍[1] 王念平[2,†]

1. 航天工程大学, 北京 101416; 2. 信息工程大学密码工程学院, 郑州 450001; † 通信作者, E-mail: wwnnpp@126.com

摘要 为评估 Piccolo 结构的密码性能, 对该结构抵抗差分密码分析和线性密码分析的能力进行研究。给出任意轮差分特征中活动轮函数和活动 S 盒个数的一个新的下界, 并利用 Piccolo 结构的差分线性对偶性, 给出任意轮线性逼近中活动轮函数和活动 S 盒个数的一个新的下界。同时, 证明这些下界是不可改进的。

关键词 Piccolo 结构; 差分密码分析; 线性密码分析

中图分类号 TN918

Further Security Evaluation for Piccolo Structure against Differential and Linear Cryptanalysis

YIN Qing[1], WANG Nianping[2,†]

1. Space Engineering University, Beijing 101416; 2. School of Cryptography Engineering, The PLA Information Engineering University, Zhengzhou 450001; † Corresponding author, E-mail: wwnnpp@126.com

Abstract To evaluate the security of Piccolo structure, the security against differential and linear cryptanalysis is investigated. A new lower bound on number of active round function and active S-boxes for arbitrary round differential characteristics is given. Using the duality between differential characteristics and linear approximations of Piccolo structure, the new lower bound on number of active round function and active S-boxes for arbitrary round linear approximations is also given. The authors prove that these lower bounds cannot be improved.

Key words Piccolo structure; differential cryptanalysis; linear cryptanalysis

对分组密码而言, 差分密码分析[1]和线性密码分析[2]是两种最重要的攻击方法, 评估分组密码抵抗这两种攻击的能力一直是密码学研究的热点。如果分组密码的最大差分特征概率(最大线性逼近概率)足够小, 就可以认为该密码对差分密码分析(线性密码分析)是安全的, 而差分特征概率(线性逼近概率)的上界通常可以用差分特征(线性逼近)中活动轮函数或活动 S 盒个数的下界来估计, 所以, 估计分组密码抵抗差分密码分析能力的关键在于求出活动轮函数或活动 S 盒个数的下界[3]。在研究差分特征中活动轮函数或活动 S 盒个数的下界时, 通常不考虑轮函数和 S 盒的具体结构, 而只假定轮函数和 S 盒是双射, 文献[4–7]就是按照此思路对不同的结构进行研究。

对于从 Piccolo 算法[8]中归纳出来的 Piccolo 结构[9], Shibutani 等[8]利用计算机模拟的方法, 给出若干轮差分特征中活动轮函数个数的下界; 殷勍等[9]利用推导证明的方法, 给出任意轮差分特征中活动轮函数个数的下界, 但没有证明此下界不可改进。

本文将推导证明与计算机模拟相结合, 在相同条件下, 改进了殷勍等[9]的结果, 并证明所得结果是不可改进的。

国家自然科学基金(61672031)资助
收稿日期: 2018–01–06; 修回日期: 2018–07–19; 网络出版日期: 2018–09–20

1 预备知识

1.1 基本概念

定义 1[10] 设 $(X,+)$ 和 $(Y,+)$ 都是有限交换群，$f:X\to Y, \alpha\in X, \beta\in Y$，令

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

则称 $p_f(\alpha\to\beta)$ 为 f 在输入差为 α 的条件下，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，“|•|”和“#{•}”表示集合的元素个数。

定义 2[10] 设 $(X,+)$ 是有限交换群，$f_{(k_1,\dots,k_n)}=f_{k_n}\dots f_{k_2}f_{k_1}$，$\alpha_1,\dots,\alpha_{n+1}\in X$，则称 $\alpha_1\to\alpha_2\to\dots\to\alpha_n\to\alpha_{n+1}$ 为 $f_{(k_1,\dots,k_n)}$ 的一个起点为 α_1，终点为 α_{n+1} 的差分传递链，并称 $p_{f_{k_1}}(\alpha_1\to\alpha_2)\cdot p_{f_{k_2}}(\alpha_2\to\alpha_3)\dots p_{f_{k_n}}(\alpha_n\to\alpha_{n+1})$ 为该差分传递链的概率。

本文也称差分传递链 $\alpha_1\to\alpha_2\to\dots\to\alpha_n\to\alpha_{n+1}$ 为 n 轮差分特征。

定义 3[10] 设 $f:Z_2^m\to Z_2^n$ 是多输出布尔函数，$\alpha=(\alpha_1,\alpha_2,\dots,\alpha_m)\in Z_2^m$，$\beta=(\beta_1,\beta_2,\dots,\beta_n)\in Z_2^n$，记

$$\rho_f(\alpha\to\beta)=W_{(\beta f)}(\alpha)=\frac{1}{2^m}\sum_{x\in Z_2^m}(-1)^{\beta\cdot f(x)\oplus\alpha\cdot x},$$

则称 $\rho_f(\alpha\to\beta)$ 为 f 在输入线性组合为 α 的条件下，输出线性组合为 β 的相关系数，称 $\alpha\to\beta$ 为 f 的一个线性逼近。其中，“⊕”表示逐位异或，“$\beta\cdot f(x)$”和“$\alpha\cdot x$”都表示点积。

定义 4[10] 设 $f_{(k_1,\dots,k_n)}=f_{k_n}\dots f_{k_2}f_{k_1}$，则称 $\alpha_1\to\alpha_2\to\dots\to\alpha_n\to\alpha_{n+1}$ 为 $f_{(k_1,\dots,k_n)}$ 的一个起点为 α_1，终点为 α_{n+1} 的组合传递链，并称 $\rho^2_{f_{(k_1,\dots,k_n)}}=\rho^2_{f_{k_1}}(\alpha_1\to\alpha_2)\cdot\rho^2_{f_{k_2}}(\alpha_2\to\alpha_3)\dots\rho^2_{f_{k_n}}(\alpha_n\to\alpha_{n+1})$ 为该组合传递链的概率。

本文也称组合传递链 $\alpha_1\to\alpha_2\to\dots\to\alpha_n\to\alpha_{n+1}$ 为 n 轮线性逼近。

显然，差分对应(线性逼近) 0→0 的概率恒为 1，因此，称 0→0 为平凡差分对应(平凡线性逼近)，否则，称为非平凡差分对应(非平凡线性逼近)。以下考虑的都是非平凡的情形。

1.2 Piccolo 结构描述

图 1 为 1 轮 Piccolo 结构，其中 $X_0,X_1,X_2,X_3\in Z_2^t$ 表示输入，f_0 和 f_1 表示轮函数，$k_0,k_1\in Z_2^t$ 表示子密钥，块移位变换 RP 表示将 4 个分块 Y_0,Y_1,Y_2,Y_3 平均分成 8 个子分块后，再对 8 个子分块进行移位变换。

为了分析方便，将 $X_i(i=0,1,2,3)$ 视为由左右规模相等的两部分 x_{2i} 和 x_{2i+1} 连接而成，表示为 $X_0=x_0\|x_1, X_1=x_2\|x_3, X_2=x_4\|x_5, X_3=x_6\|x_7$，则 Piccolo 结构的输入可表示为 $(x_0\|x_1,x_2\|x_3,x_4\|x_5,x_6\|x_7)\in(Z_2^{t/2})^8$，故 1 轮 Piccolo 结构(略去子密钥)可表示为

$$\begin{aligned}&Q(x_0\|x_1,x_2\|x_3,x_4\|x_5,x_6\|x_7)\\&\quad=\mathrm{RP}(x_0\|x_1,f_0(x_0\|x_1)\oplus x_2\|x_3,\\&\qquad x_4\|x_5,f_1(x_4\|x_5)\oplus x_6\|x_7)。\end{aligned}$$

1) 轮函数 f_0 和 f_1。如图 2 所示，轮函数 f_0 和 f_1 都采用 SPS 结构，其中，S 表示 n 个 m 比特双射 S 盒的并置(n 为偶数，$nm=t$，t 表示输入块 $X_i(i=0,1,2,3)$ 的比特位数)，P 表示线性变换 $P:(Z_2^m)^n\to(Z_2^m)^n$，$\boldsymbol{x}\to\boldsymbol{M}\cdot\boldsymbol{x}$，$\boldsymbol{x}$ 是列向量，$\boldsymbol{M}$ 是有限域 GF(2^m) 上的 n 阶 MDS 矩阵。显然，P 变换的差分分支数[10]和线性分支数[10]都为 n+1，且轮函数 f_0 和 f_1 都为双射。

2) 块移位变换 RP。如图 3 所示，设块移位变换 RP 的输入为 $y=(Y_0,Y_1,Y_2,Y_3)=(y_0,y_1,y_2,y_3,y_4,y_5,y_6,y_7)\in(Z_2^{t/2})^8$，则块移位变换 RP 可表示为 $\mathrm{RP}(y)=\mathrm{RP}(y_0,y_1,y_2,y_3,y_4,y_5,y_6,y_7)=(y_2,y_7,y_4,y_1,y_6,y_3,y_0,y_5)$。

定义 5[11] 设 $\alpha\to\beta$ 是轮函数(S 盒)的一个差分对应，若 $\alpha\neq 0$，则称该轮函数(S 盒)为差分活动轮函数(S 盒)。

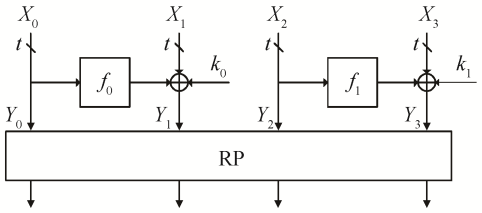

图 1 Piccolo 结构
Fig. 1 Piccolo structure

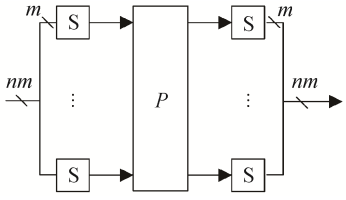

图 2 轮函数
Fig. 2 Round function

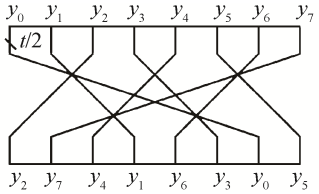

图 3　块移位变换 RP
Fig. 3　Block shift transformation RP

性质 1[9]　对于 Piccolo 结构的轮函数 $f_j(j=0,1)$，设 $\alpha\to\gamma\to\delta\to\beta$ 是轮函数 $f_j(j=0,1)$ 的差分对应，$\alpha_0,\alpha_1,...,\alpha_{n-1}$，$\gamma_0,\gamma_1,...,\gamma_{n-1}$，$\delta_0,\delta_1,...,\delta_{n-1}$ 和 $\beta_0,\beta_1,...,\beta_{n-1}$ 依次为 α,γ,δ 和 β 的 n 个分块，且 $\alpha_j\to\gamma_j$ 或 $\delta_j\to\beta_j(\forall j,0\le j\le n-1)$ 表示 S 变换的第 j 个 S 盒的差分对应，$(\gamma_0,\gamma_1,...,\gamma_{n-1})\to(\delta_0,\delta_1,...,\delta_{n-1})$ 是 P 变换的差分对应。对于 $\forall\boldsymbol{\alpha}=(\alpha_0,\alpha_1,...,\alpha_{n-1})\in(Z_2^m)^n$，将 $\boldsymbol{\alpha}$ 看成 $Z_2^{mn/2}$ 上的 2 维列向量，即 $\boldsymbol{\alpha}=(\alpha_0,\alpha_1)\in(Z_2^{mn/2})^2$，并将 α_0,α_1 中非零元的个数记为 $W(\boldsymbol{\alpha})$，则对于 $f_j:(Z_2^{mn/2})^2\to(Z_2^{mn/2})^2$ 的差分对应 $\alpha\to\beta$，有 $\min\limits_{0\ne a\in(Z_2^{mn/2})^2}\{W(\alpha)+W(\beta)\}=3$。

2　轮函数和活动 S 盒个数下界

2.1　差分活动轮函数和活动 S 盒个数下界

设 $(\alpha_0\|\alpha_1,\alpha_2\|\alpha_3,\alpha_4\|\alpha_5,\alpha_6\|\alpha_7)$ 是 Piccolo 结构的输入差分，“1”代表非零差分块 α_i，“0”代表零差分块 α_i $(i=0,1,2,...,7)$，则 Piccolo 结构非零输入差分有且仅有 2^8–1=255 种表示，即 $\Delta_1=(10000000)\overset{\text{def}}{=}1$，$\Delta_2=(01000000)\overset{\text{def}}{=}2,...,\Delta_{255}=(11111111)\overset{\text{def}}{=}255$。若左起第 1 和 2 位不全为零，则 f_0 为活动轮函数；若第 5 和 6 位不全为零，则 f_1 为活动轮函数。

首先，给出输入输出差分块“1”和“0”通过 XOR 运算和轮函数需要满足的约束条件。令 $a,b,c,d\in\{0,1\}$ 分别代表 $\alpha,\beta,\gamma,\delta\in Z_2^{t/2}$，“∧”表示按位与，“∨”表示按位或。

条件 1　差分经过 XOR 运算时满足以下条件：设 $\alpha\oplus\beta=\gamma$，则

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

条件 1 表示，对于 $\alpha\oplus\beta=\gamma$，当 α 和 β 至少有一个为零时，有 $c=a+b$；当 α 和 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。

条件 2　差分经过轮函数时满足以下条件：设 $f(\alpha\|\beta)=\gamma\|\delta$，则

$$a+b+c+d\begin{cases}\ge 3, & \text{当}a\vee b=1,\\ =0, & \text{当}a=b=0。\end{cases}$$

条件 2 表示，当轮函数输入差分非零时，因为输入差分和输出差分满足性质 1，所以 $a+b+c+d\ge 3$；当轮函数输入差分为零时，输出差分也为零。

以条件 1 和 2 作为约束，对于 Piccolo 结构，当给定输入差分的“0”和“1”表示和迭代轮数时，通过计算机搜索，容易给出输出差分的“0”和“1”表示及其所需活动轮函数个数的最小值。利用这两个约束条件可以完成以下 3 个实验。

实验 1　通过计算机搜索，给出 6 轮差分特征中活动轮函数个数的最小值。

实验结果如图 4 所示，其中第 x 行第 y 列(x 和 y 都是十六进制)交叉处的数值表示以 Δ_{xy} 为首轮差分输入的 6 轮差分特征中活动轮函数个数的最小值。例如，第 3 行第 e 列交叉处的数值为 7，就表示以 $\Delta_{xy}=\Delta_{3e}=(3\,e)=(\underline{1100}\,\underline{0111})$ 为首轮差分输入的 6 轮差分特征中活动轮函数个数的最小值为 7。这里，$3=\underline{1100}=1\times2^0+1\times2^1+0\times2^2+0\times2^3$，$e=\underline{0111}=0\times2^0+1\times2^1+1\times2^2+1\times2^3$，且行数和列数都从 0 开始统计。

从图 4 可得以下结论。

命题 1　对于 Piccolo 结构，任一 6 轮差分特征至少有 6 个活动轮函数。

实验 2　通过计算机搜索，筛选出所有恰有 6 个活动轮函数的 6 轮差分特征的尾轮输出差分(十六进制)，筛选结果记为集合 A，表示如下(不计重复值)。

3	13	15	17	19	23	26	2a	2b	30
31	32	33	36	39	4a	4b	51	58	59
5b	5e	5f	62	63	67	6a	6b	71	76
77	78	79	7a	7b	7e	7f	85	87	91
93	95	97	9b	a2	a4	a6	a7	ad	af
b2	b4	b5	b6	b7	b9	bb	bd	bf	da
db	e5	e7	f5	f7	fa	fb			

实验 3　对于 $k=1,2,3,4,5$，通过计算机搜索，筛选出所有恰有 $k-1$ 个活动轮函数的 k 轮差分特征的首轮输入差分(十六进制)，筛选结果记为集合 B，如下表示(不计重复值)。

4	7	8	b	c	d	e	f	40	44
45	48	4c	4d	54	70	80	84	88	8a
8c	8e	a8	b0	c0	c4	c8	cc	d0	d4
e0	e8	f0							

通过观察发现，集合 A 和 B 没有公共元素，故

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	–	8	7	7	7	7	7	6	6	8	7	6	7	7	6	6
1	8	8	8	8	8	8	8	8	7	8	8	8	7	8	8	8
2	7	8	8	8	7	8	8	8	7	8	8	8	7	8	8	8
3	7	8	7	7	6	7	7	7	6	7	7	7	7	7	7	7
4	7	8	7	6	7	7	6	6	6	8	6	6	7	7	6	6
5	7	8	8	7	6	8	8	7	7	7	7	7	7	7	7	7
6	7	8	7	7	6	8	7	7	7	7	7	7	7	7	7	7
7	6	7	7	7	6	7	7	7	6	7	7	7	6	7	7	7
8	6	8	7	6	6	8	7	6	7	7	6	6	7	7	6	6
9	8	8	8	7	8	7	7	7	6	8	7	7	7	7	7	7
a	7	8	8	7	7	7	7	7	6	8	7	7	7	7	7	7
b	6	7	7	7	6	7	7	7	6	7	7	7	6	7	7	7
c	7	7	7	7	7	7	7	7	6	7	7	7	6	7	7	7
d	7	8	8	7	6	7	7	7	6	7	7	7	7	7	7	7
e	6	8	7	6	6	7	6	6	6	7	7	6	7	7	6	6
f	6	7	7	7	6	7	7	7	6	7	7	7	6	7	7	7

图 4 6 轮差分特征中活动轮函数个数的最小值

Fig. 4 Minimum of number of active round function for 6-round differential characteristics

可得以下结论。

命题 2 对于 Piccolo 结构，任一恰有 6 个活动轮函数的 6 轮差分特征后面不可能“联接”一个恰有 $k-1$ $(k=1,2,3,4,5)$ 个活动轮函数的 k 轮差分特征。

引理 1 对于 Piccolo 结构，设 $\alpha^{(0)}\to\alpha^{(1)}\to\ldots\to\alpha^{(6)}\to\ldots\to\alpha^{(6n-6)}\to\ldots\to\alpha^{(6n)}$ 为任一恰有 $6n$ 个活动轮函数的 $6n$ 轮差分特征，则最后 6 轮差分特征 $\alpha^{(6n-6)}\to\ldots\to\alpha^{(6n)}$ 恰有 6 个活动轮函数。

证明 根据命题 1 可知，6 轮差分特征 $\alpha^{(6n-6)}\to\ldots\to\alpha^{(6n)}$ 至少有 6 个活动轮函数。若 $\alpha^{(6n-6)}\to\ldots\to\alpha^{(6n)}$ 中活动轮函数的个数大于 6，则 $6(n-1)$ 轮差分特征 $\alpha^{(0)}\to\alpha^{(1)}\to\ldots\to\alpha^{(6)}\to\ldots\to\alpha^{(6n-6)}$ 中活动轮函数的个数必小于 $6(n-1)$，与命题 1 相矛盾，故 $\alpha^{(6n-6)}\to\ldots\to\alpha^{(6n)}$ 必含有 6 个活动轮函数，所以本结论成立。

定理 1[9] 对于 Piccolo 结构，k $(k\geq 1)$ 轮差分特征至少有 $k-1$ 个活动轮函数。

定理 2 对于 Piccolo 结构，以下结论成立。

1) k $(1\leq k\leq 5)$ 轮差分特征至少有 $k-1$ 个活动轮函数。

2) k $(k\geq 6)$ 轮差分特征至少有 k 个活动轮函数。

证明 1) 由定理 1，即知。2) 当 $k=6s$ $(s\geq 1)$ 时，由命题 1 可知，本结论成立。当 $k=6s+m$ $(s\geq 1, 1\leq m\leq 5)$ 时，分以下两种情形进行讨论。

情形 1: 当前 $6s$ 轮差分特征至少有 $6s+1$ 个活动轮函数时，由定理 1 可知，后 m 轮差分特征至少有 $m-1$ 个活动轮函数，所以 $6s+m$ 轮差分特征至少有 $(6s+1)+(m-1)=6s+m$ 个活动轮函数。

情形 2: 当前 $6s$ 轮差分特征恰有 $6s$ 个活动轮函数时，设 $\alpha^{(0)}\to\ldots\to\alpha^{(6s)}\to\ldots\to\alpha^{(6s+m)}$ 为任一 $6s+m$ 轮差分特征，且 $6s$ 轮差分特征 $\alpha^{(0)}\to\ldots\to\alpha^{(6s)}$ 恰有 $6s$ 个活动轮函数。由引理 1 知，$\alpha^{(6s-6)}\to\ldots\to\alpha^{(6s)}$ 恰有 6 个活动轮函数，再由命题 2 和定理 1 可知，后 m 轮差分特征 $\alpha^{(6s)}\to\ldots\to\alpha^{(6s+m)}$ 至少有 m 个活动轮函数，所以 $6s+m$ 轮差分特征至少有 $6s+m$ 个活动轮函数。

结合轮函数中 P 变换的差分分支数[10]为 $(n+1)$，由定理 2 可得以下结论。

推论 1 对于 Piccolo 结构，以下结论成立。

1) $k(5\geq k\geq 1)$ 轮差分特征至少有 $(n+1)(k-1)$ 个活动 S 盒。

2) $k(k\geq 6)$ 轮差分特征至少有 $(n+1)k$ 个活动 S 盒。

2.2 线性活动轮函数和活动 S 盒个数的下界

定义 6[9] 若 $\mathcal{R}$ 满足以下两个条件，则称密码结构 $\mathcal{R}$ 具有差分–线性对偶性。

1) 对任一活动轮函数个数为 s $(s\geq 0)$ 的 k 轮差分特征 U，都存在活动轮函数个数为 s $(s\geq 0)$ 的 k 轮线性逼近 U^*。

2) 对任一活动轮函数个数为 s ($s \ge 0$) 的 k 轮线性逼近 U^*，都存在活动轮函数个数为 s ($s \ge 0$) 的 k 轮差分特征 U。

定理 3[9]　Piccolo 结构具有差分–线性对偶性。

定理 4　对于 Piccolo 结构，以下结论成立。

1) k ($1 \le k \le 5$) 轮线性逼近至少有 $k-1$ 个活动轮函数;

2) k ($k \ge 6$) 轮线性逼近至少有 k 个活动轮函数。

证明　由定理 2 和 3 易知本结论成立。

结合轮函数中 P 变换的线性分支数[10]为(n+1)，由定理 4 可得到以下推论。

推论 2　对于 Piccolo 结构，以下结论成立。

1) k ($1 \le k \le 5$) 轮线性逼近至少有 $(n+1)(k-1)$ 个活动 S 盒。

2) k ($k \ge 6$) 轮线性逼近至少有 $(n+1)k$ 个活动 S 盒。

定理 5　设 S 盒的最大差分概率和最大线性逼近概率分别为 p 和 q，则以下结论成立。

1) k ($1 \le k \le 5$) 轮 Piccolo 结构的最大差分特征概率 $\le p^{(n+1)(k-1)}$，最大线性逼近概率 $\le q^{(n+1)(k-1)}$。

2) k ($k \ge 6$) 轮 Piccolo 结构的最大差分特征概率 $\le p^{(n+1)k}$，最大线性逼近概率 $\le q^{(n+1)k}$。

2.3　Piccolo 结构活动轮函数个数下界的不可改进性

本节证明，定理 2 和 4 给出的活动轮函数个数的下界是不可改进的，即确实存在一类差分特征和线性逼近，其活动轮函数的个数恰好达到给出的下界。

设 $\alpha, \beta, \gamma, \delta, \eta, \varepsilon$ 全不为零。为叙述方便，用 S_1 表示 2 轮差分特征 $(0\|0,\ \alpha\|0,\ 0\|0,\ 0\|0) \to (\alpha\|0,\ 0\|0,\ 0\|0,\ 0\|0) \to (\beta\|0,\ 0\|0,\ 0\|\gamma,\ \alpha\|0)$，其轮函数差分对应依次为 $f_0^{(1)}: 0 \to 0$, $f_1^{(1)}: 0 \to 0$, $f_0^{(2)}: \alpha\|0 \to \beta\|\gamma$, $f_1^{(2)}: 0 \to 0$。

用 S_2 表示 3 轮差分特征 $(\alpha\|\beta, \gamma\|0, 0\|0, 0\|0) \to (0\|0, 0\|\beta, 0\|0, \alpha\|0) \to (0\|0, 0\|0, \alpha\|\beta, 0\|0) \to (0\|0, \alpha\|0, \gamma\|0, 0\|\beta)$，其轮函数差分对应依次为 $f_0^{(1)}: \alpha\|\beta \to \gamma\|0$, $f_1^{(1)}: 0 \to 0$, $f_0^{(2)}: 0 \to 0$, $f_1^{(2)}: 0 \to 0$, $f_0^{(3)}: 0 \to 0$, $f_1^{(3)}: \alpha\|\beta \to \gamma\|0$。

用 S_3 表示 4 轮差分特征 $(\alpha\|\beta, \gamma\|0, 0\|0, 0\|0) \to (0\|0, 0\|\beta, 0\|0, \alpha\|0) \to (0\|0, 0\|0, \alpha\|\beta, 0\|0) \to (0\|0, \alpha\|0, \gamma\|0, 0\|\beta) \to (\alpha\|\delta, \gamma\|0, \alpha\|0, 0\|0)$，其轮函数差分对应依次为 $f_0^{(1)}: \alpha\|\beta \to \gamma\|0$, $f_1^{(1)}: 0 \to 0$, $f_0^{(2)}: 0 \to 0$, $f_1^{(2)}: 0 \to 0$, $f_0^{(3)}: 0 \to 0$, $f_1^{(3)}: \alpha\|\beta \to \gamma\|0$, $f_0^{(4)}: 0 \to 0$, $f_1^{(4)}: \gamma\|0 \to \alpha\|\delta \oplus \beta$，其中 $\delta \oplus \beta \ne 0$。

用 S_4 表示 5 轮差分特征 $(\alpha\|0, \gamma\|0, 0\|0, \delta\|0) \to (0\|0, 0\|0, \delta\|\beta, \alpha\|0) \to (0\|0, \delta\|0, 0\|0, 0\|\beta) \to (\delta\|\beta, 0\|0, 0\|0, 0\|0) \to (\alpha\|0, 0\|\beta, 0\|0, \delta\|0) \to (\delta\|0, 0\|0, \delta\|0, \alpha\|0,)$，其轮函数差分对应依次为 $f_0^{(1)}: \alpha\|0 \to \gamma\|\beta$, $f_1^{(1)}: 0 \to 0$, $f_0^{(2)}: 0 \to 0$, $f_1^{(2)}: \delta\|\beta \to \alpha\|0$, $f_0^{(3)}: 0 \to 0$, $f_1^{(3)}: 0 \to 0$, $f_0^{(4)}: \delta\|\beta \to \alpha\|0$, $f_1^{(4)}: 0 \to 0$, $f_0^{(5)}: \alpha\|0 \to \delta\|\beta$, $f_1^{(5)}: 0 \to 0$。

由 $\alpha, \beta, \gamma, \delta, \varepsilon, \eta \ne 0$ 可知，S_1 有 1 个活动轮函数，S_2 有 2 个活动轮函数，S_3 有 3 个活动轮函数，S_4 有 4 个活动轮函数。这说明，对 $k = 2, 3, 4, 5$，定理 2第1个结论中活动轮函数个数的下界是不可改进的。又因为 $k = 1$ 时，显然存在恰有 0 个活动轮函数的 1 轮差分特征，所以定理 2 第 1 个结论中的下界是不可改进的，再由定理 3 知，定理 4 第 1 个结论中的下界也是不可改进的。

下面说明定理 2 第 2 个结论和定理 4 第 2 个结论中的下界是不可改进的。

S_5 表示 3 轮差分特征 $(0\|0, \alpha\|0, \beta\|\gamma, 0\|\delta) \to (\alpha\|\eta, \beta\|0, 0\|0, 0\|\gamma) \to (\varepsilon\|\gamma, 0\|\eta, 0\|0, \alpha\|0) \to (0\|0, 0\|\gamma, \alpha\|\delta, \varepsilon\|0)$，其轮函数差分对应依次为 $f_0^{(1)}: 0 \to 0$, $f_1^{(1)}: \beta\|\gamma \to 0\|\delta \oplus \eta$, $f_0^{(2)}: \alpha\|\eta \to \beta \oplus \varepsilon\|0$, $f_1^{(2)}: 0 \to 0$, $f_0^{(3)}: \varepsilon\|\gamma \to 0\|\eta \oplus \delta$, $f_1^{(3)}: 0 \to 0$, 其中 $\delta \oplus \eta$, $\beta \oplus \varepsilon$ 和 $\eta \oplus \delta$ 都不为零。

S_5 的每一轮各含有 1 个活动轮函数。现在将两个 S_5 “联接”在一起得到 $S_5 \to S_5$，其中“联接”处的差分特征 $(0\|0, 0\|\gamma, \alpha\|\delta, \varepsilon\|0) \to (0\|0, \alpha\|0, \beta\|\gamma, 0\|\delta)$ 的轮函数差分对应为 $f_0^{(4)}: 0 \to 0$, $f_0^{(3)}: \alpha\|\delta \to \varepsilon \oplus \beta\|0$，其中 $\varepsilon \oplus \beta \ne 0$。易知，$S_5 \to S_5$ 的每一轮各含有 1 个活动轮函数。这样一来，通过“联接” S_5，可以得到任意 k ($k \ge 1$) 轮有 k 个活动轮函数的差分特征，故定理 2 第 2 个结论中的下界是不可改进的，再由定理 3 知，定理 4 第 2 个结论中的下界也是不可改进的。

3　结束语

本文给出 Piccolo 结构抵抗差分密码分析和线性密码分析能力的评估结果。具体地，给出任意轮差分特征中活动轮函数和活动 S 盒个数的一个新下界，并利用差分线性对偶性，给出任意轮线性逼近中活动轮函数和活动 S 盒个数的一个新下界。本研

究的意义在于, 仅需要计算 S 盒的最大差分概率(最大线性逼近概率), 就可以给出差分特征(线性逼近)概率的上界, 进而估计出密码算法抵抗差分密码分析(线性密码分析)的安全性。本文的研究结果对于利用 Piccolo 结构设计新的密码算法具有重要的指导意义。下一步, 将研究 Piccolo 结构抵抗其他攻击方法的安全性。

参考文献

[1] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems // CRYPTO'90 Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology. Berlin, 1991: 2–21

[2] Matsui M. Linear cryptanalysis method for DES cipher // Advances in Cryptology—EUROCRYPT'93, LNCS 765. Lofthus, 1994: 386–397

[3] Knudsen L R. Practically secure Feistel ciphers // Fast Software Encryption'93, LNCS 806. Cambridge, 1994: 211–221

[4] 吴文玲, 贺也平. 一类广义 Feistel 密码的安全性评估. 电子与信息学报, 2002, 24(9): 1177–1184

[5] Wang Q Y, Zhang B, Jin C H. Practical Security against differential and linear cryptanalysis for SMS4-like cipher. Journal of Networks, 2013, 8(8): 1689–1693

[6] 王念平. 一类广义 Feistel 密码的安全性能分析. 大连海事大学学报, 2007, 33(3): 63–67

[7] Zhao G, Cheng L, Li C, et al. On the practical security bound of GF-NLFSR structure with SPN round function // Provable Security 2014, LNCS 8782. Hong Kong, 2014: 40–54

[8] Shibutani K, Isobe T, Hiwatari H, et al. Piccolo: an ultra-lightweight block cipher // Cryptographic Hardware and Embedded Systems—CHES 2011, LNCS 6917. Nara, 2011: 342–357

[9] 殷勍, 王念平. Piccolo 结构抵抗差分和线性密码分析能力评估. 山东大学学报(理学版), 2016, 51(3): 132–142

[10] 金晨辉, 郑浩然, 张少武, 等. 密码学. 北京: 高等教育出版社, 2009

[11] Schneier B, Kelsey J. Unbalanced Feistel networks and block cipher design // Fast Software Encryption' 95, LNCS 3557. Cambridge, 1996: 121–144