一类特殊的比特变换的研究

王念平
(解放军信息工程大学电子技术学院,河南郑州 450004)

摘 要: 在S-P网络中,P变换的设计直接影响着分组密码的整体扩散性能.基于此,提出了一类特殊的比特变换的概念,证明了该类比特变换是对合变换且其分支数为4,并给出了输入和输出重量之和等于4的输入输出对的个数.进一步的分析表明,尽管该类比特变换的分支数没有达到最大值,但仍然具有较好的扩散性能.

关键词: 一类特殊的比特变换; 对合变换; 分支数; 扩散性
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2012) 04-0838-04
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.04.035

Researches on A Class of Special Bit Transformation

WANG Nian-ping
(*Institute of Electronic Technology, the PLA Information Engineering University, Zhengzhou, Henan* 450004, *China*)

Abstract: In the S-P networks, the design of P-transformation is very important, and is related to integral diffusion performance of block cipher. Based on the importance of P transformation, we propose the concept of a class of special bit transformation. We prove that the special bit transformation is involutory transformation and it's branch number is 4. We also give the number of input-output correspondences whose weight sum equals to 4. By further analyzing, it is shown that the special bit transformation has good diffusion performance though it's branch number does not obtain maximum.

Key words: a class of special bit transformation; involutory transformation; branch number; diffusion performance

1 引言

"混乱"和"扩散"是分组密码设计的一般原则.在代替-置换网络(简称S-P网络)中,P变换的设计是非常重要的,它直接影响着分组密码的整体扩散性能[1,2].P变换可以设计成有限域上的线性变换[3,4],特别地,P变换可以设计成二元域上的线性变换[5,6].P变换也可以设计成模2^n剩余类环上的线性变换[7,8].此外,P变换还可以设计成环$(Z_2^n, \oplus, \wedge)$上的线性变换,例如Crypton[9]的扩散层就是典型的例子.P变换的最后一种设计方法只用逐比特逻辑与运算和逐比特模2加运算即可实现,相当简单有效.基于此,本文提出了一类特殊的比特变换的概念并对其进行了详细的研究.

为方便起见,以下用Z_2表示二元域,用Z_2^n表示Z_2上的n维向量之集合,用$(Z_2^n)^4$表示Z_2^n上的4维向量之集合;用"$\wedge$"和"$\oplus$"分别表示Z_2^n中元素的逐比特逻辑与和逐比特模2加;用"T"表示矩阵(或向量)的转置,用$Hankel(c_0, c_1, c_2, c_3)$表示$Z_2^n$上如下形式的矩阵

$$\begin{pmatrix} c_0 & c_1 & c_2 & c_3 \\ c_1 & c_2 & c_3 & c_0 \\ c_2 & c_3 & c_0 & c_1 \\ c_3 & c_0 & c_1 & c_2 \end{pmatrix}$$

并用"E"表示Z_2上的单位矩阵;对$\forall\ a = a_{n-1}a_{n-2}\cdots a_0 \in Z_2^n$,称$a_j(0\leqslant j\leqslant n-1)$为$a$的第$j$比特(注意,这里的$j$从零开始计).对$\forall\ (a_0, a_1, a_2, a_3)\in (Z_2^n)^4$,重量$W(a_0, a_1, a_2, a_3)$表示$(a_0, a_1, a_2, a_3)$中非零分量$a_j(0\leqslant j\leqslant 3)$的个数.

2 有关的定义和引理

定义1 设$a = a_{n-1}a_{n-2}\cdots a_0, b = b_{n-1}b_{n-2}\cdots b_0, c = c_{n-1}c_{n-2}\cdots c_0 \in Z_2^n$.若$\forall\ i, 0\leqslant i\leqslant n-1, c_i = a_i\cdot b_i$,则称$c$为$a$和$b$的逐比特逻辑与,记作$c = a\wedge b$.其中,"$\cdot$"表示$Z_2$中的乘法.

定义2 设$c_i\in Z_2^n, 0\leqslant i\leqslant 3$,称$(Z_2^n)^4\rightarrow(Z_2^n)^4$的变换$(a_0, a_1, a_2, a_3)\rightarrow(b_0, b_1, b_2, b_3)$:

收稿日期:2010-07-03;修回日期:2011-03-07
基金项目:河南省信息安全重点实验室基金(No.9140C1102060702)

$$b_i = c_i \wedge a_0 \oplus c_{(i+1)\bmod 4} \wedge a_1 \oplus c_{(i+2)\bmod 4} \wedge a_2 \oplus c_{(i+3)\bmod 4} \wedge a_3 (0 \leqslant i \leqslant 3)$$

为 Z_2^n 上基于逐比特逻辑与运算的比特变换,简称 Z_2^n 上的比特变换,并记作 $(a_0, a_1, a_2, a_3) \xrightarrow{\wedge(c_0, c_1, c_2, c_3)} (b_0, b_1, b_2, b_3)$.

易知,Z_2^n 上基于逐比特逻辑与运算的比特变换实质上是环 $(Z_2^n, \oplus, \wedge)$ 上的线性变换 $(b_0, b_1, b_2, b_3)^{\mathrm{T}} = Hankel(c_0, c_1, c_2, c_3) \wedge (a_0, a_1, a_2, a_3)^{\mathrm{T}}$.

定义 3 设 $c_i = c_{i(n-1)} c_{i(n-2)} \cdots c_{i0} \in Z_2^n, 0 \leqslant i \leqslant 3$,且设 $A_1 = Hankel(0,1,1,1)$, $A_2 = Hankel(1,0,1,1)$, $A_3 = Hankel(1,1,0,1)$, $A_4 = Hankel(1,1,1,0)$. 若 $\forall j, 0 \leqslant j \leqslant n-1, C_j \in \{A_1, A_2, A_3, A_4\}$,则称比特变换 $(a_0, a_1, a_2, a_3) \xrightarrow{\wedge(c_0, c_1, c_2, c_3)} (b_0, b_1, b_2, b_3)$ 为 Z_2^n 上一类特殊的比特变换.

Crypton[9]扩散层中的变换 π_0 和 π_1 就是 Z_2^{32} 上的一类特殊的比特变换.

定义 4 设 $c_i \in Z_2^n, 0 \leqslant i \leqslant 3$,若 $\forall (a_0, a_1, a_2, a_3) \in (Z_2^n)^4$,有 $(a_0, a_1, a_2, a_3) \xrightarrow{\wedge(c_0, c_1, c_2, c_3)} (b_0, b_1, b_2, b_3) \xrightarrow{\wedge(c_0, c_1, c_2, c_3)} (a_0, a_1, a_2, a_3)$ 成立,则称比特变换

$$(a_0, a_1, a_2, a_3) \xrightarrow{\wedge(c_0, c_1, c_2, c_3)} (b_0, b_1, b_2, b_3)$$

是对合的,简称对合型比特变换.

定义 5 称 $B_F = \min_{(a_0, a_1, a_2, a_3) \neq (0,0,0,0)} (W(a_0, a_1, a_2, a_3) + W(b_0, b_1, b_2, b_3))$ 为比特变换 $(a_0, a_1, a_2, a_3) \xrightarrow{\wedge(c_0, c_1, c_2, c_3)} (b_0, b_1, b_2, b_3)$ 的分支数.

3 主要结论

定理 1 Z_2^n 上一类特殊的比特变换 $(a_0, a_1, a_2, a_3) \xrightarrow{\wedge(c_0, c_1, c_2, c_3)} (b_0, b_1, b_2, b_3)$ 是对合型比特变换.

证明 容易验证 $A_1^2 = A_2^2 = A_3^2 = A_4^2 = E$,而 $C_j \in \{A_1, A_2, A_3, A_4\}$,故 $C_j^2 = E$,从而对 $\forall (a_0, a_1, a_2, a_3) \in (Z_2^n)^4$,有 $(a_0, a_1, a_2, a_3) \xrightarrow{\wedge(c_0, c_1, c_2, c_3)} (b_0, b_1, b_2, b_3) \xrightarrow{\wedge(c_0, c_1, c_2, c_3)} (a_0, a_1, a_2, a_3)$ 成立,亦即 $(a_0, a_1, a_2, a_3) \xrightarrow{\wedge(c_0, c_1, c_2, c_3)} (b_0, b_1, b_2, b_3)$ 是对合型比特变换.

证毕

定理 2 Z_2^n 上一类特殊的比特变换 $(a_0, a_1, a_2, a_3) \xrightarrow{\wedge(c_0, c_1, c_2, c_3)} (b_0, b_1, b_2, b_3)$ 的分支数等于 4.

证明 由定理 1 知,一类特殊的比特变换 $(a_0, a_1, a_2, a_3) \xrightarrow{\wedge(c_0, c_1, c_2, c_3)} (b_0, b_1, b_2, b_3)$ 是可逆的,故其分支数 $\geqslant 2$.

先证其分支数 $\neq 2$.(反证法)

若其分支数 = 2,则由一类特殊的比特变换的可逆性知,必存在 $(a_0, a_1, a_2, a_3) \in (Z_2^n)^4$,使得 $W(a_0, a_1, a_2, a_3) = W(b_0, b_1, b_2, b_3) = 1$. 不妨设 $a_0 \neq 0, a_1 = a_2 = a_3 = 0$. 由比特变换的定义知 $b_i = c_i \wedge a_0 \oplus c_{(i+1)\bmod 4} \wedge 0 \oplus c_{(i+2)\bmod 4} \wedge 0 \oplus c_{(i+3)\bmod 4} \wedge 0 = c_i \wedge a_0 (0 \leqslant i \leqslant 3)$.

因 $a_0 \neq 0$,故不妨再设 $a_{0j} = 1 (0 \leqslant j \leqslant n-1)$,从而由一类特殊的比特变换的定义知

$$\begin{aligned} W(b_0, b_1, b_2, b_3) &= W(c_0 \wedge a_0, c_1 \wedge a_0, c_2 \wedge a_0, c_3 \wedge a_0) \\ &\geqslant W(c_{0j} \cdot a_{0j}, c_{1j} \cdot a_{0j}, c_{2j} \cdot a_{0j}, c_{3j} \cdot a_{0j}) \\ &= W(c_{0j}, c_{1j}, c_{2j}, c_{3j}) \\ &= 3 \end{aligned}$$

这与 $W(b_0, b_1, b_2, b_3) = 1$ 矛盾,故其分支数 $\neq 2$. 其中,最后一步 $W(c_{0j}, c_{1j}, c_{2j}, c_{3j}) = 3$ 用到了定义 3.

类似地,可证其分支数 $\neq 3$ 和其分支数 $\leqslant 4$,从而其分支数必等于 4. 证毕

设 $(\alpha_0, \alpha_1, \alpha_2, \alpha_3)^{\mathrm{T}} \in (Z_2^n)^4$ 为一类特殊的比特变换 $(a_0, a_1, a_2, a_3) \xrightarrow{\wedge(c_0, c_1, c_2, c_3)} (b_0, b_1, b_2, b_3)$ 的任一输入,$(\beta_0, \beta_1, \beta_2, \beta_3)^{\mathrm{T}} \in (Z_2^n)^4$ 为相应的输出,设 $W(\alpha_0, \alpha_1, \alpha_2, \alpha_3) = i, W(\beta_0, \beta_1, \beta_2, \beta_3) = j (1 \leqslant i, j \leqslant 4)$. 此时,为方便起见,称满足条件 $W(\alpha_0, \alpha_1, \alpha_2, \alpha_3) + W(\beta_0, \beta_1, \beta_2, \beta_3) = 4$ 和 $W(\alpha_0, \alpha_1, \alpha_2, \alpha_3) = i, W(\beta_0, \beta_1, \beta_2, \beta_3) = j (1 \leqslant i, j \leqslant 4)$ 的输入输出对 $(\alpha_0, \alpha_1, \alpha_2, \alpha_3)^{\mathrm{T}} \rightarrow (\beta_0, \beta_1, \beta_2, \beta_3)^{\mathrm{T}}$ 为达到最小扩散的"$i \rightarrow j$"型输入输出对.

定理 2 指出,一类特殊的比特变换 $(a_0, a_1, a_2, a_3) \xrightarrow{\wedge(c_0, c_1, c_2, c_3)} (b_0, b_1, b_2, b_3)$ 的分支数为 4,而不是最大值 5. 但以下的几个定理表明,达到最小扩散的输入输出对的数量是相当有限的,从而该类比特变换具有较好的扩散性.

对 A_1, A_2, A_3, A_4 而言,以下几个性质成立.

性质 1 $W(\xi) = 1$ 时必有 $W(A_i \xi^{\mathrm{T}}) = 3$ 成立;$W(\xi) = 2$ 时必有 $W(A_i \xi^{\mathrm{T}}) = 2$ 成立;$W(\xi) = 3$ 时必有 $W(A_i \xi^{\mathrm{T}}) = 1$ 成立.

性质 2 对 $\forall \xi = (\xi_0, \xi_1, \xi_2, \xi_3) \in Z_2^4, W(\xi) = 1$,必有 $A_i \xi^{\mathrm{T}} \neq A_j \xi^{\mathrm{T}} (\forall i, j, i \neq j, 1 \leqslant i, j \leqslant 4)$ 成立.

性质 3 当 $\xi \in \{(1,1,0,0), (0,1,1,0), (0,0,1,1), (1,0,0,1)\}$ 时,必有 $A_i \xi^{\mathrm{T}} \neq A_j \xi^{\mathrm{T}} (\forall i, j, i \neq j, 1 \leqslant i, j \leqslant 4)$ 成立.

性质 4 当 $\xi \in \{(1,0,1,0), (0,1,0,1)\}$ 时,必有 $A_1 \xi^{\mathrm{T}} = A_3 \xi^{\mathrm{T}}, A_2 \xi^{\mathrm{T}} = A_4 \xi^{\mathrm{T}}$ 成立.

设矩阵 $C_0, C_1, \cdots, C_{n-1} (C_j (0 \leqslant j \leqslant n-1)$ 的含义如定义 3 所示)中 A_1, A_2, A_3, A_4 的个数分别为 $N_1, N_2, N_3, N_4, N_1 + N_2 + N_3 + N_4 = n$. 为方便,设 $C_0 = \cdots = C_{N_1 - 1} = A_1, C_{N_1} = \cdots = C_{N_1 + N_2 - 1} = A_2$,

$$C_{N_1+N_2}=\cdots=C_{N_1+N_2+N_3-1}=A_3,\ C_{N_1+N_2+N_3}=\cdots=C_{n-1}=A_4.$$

再设一类特殊的比特变换的输入为$(\alpha_0,\alpha_1,\alpha_2,\alpha_3)^{\mathrm{T}}\in(Z_2^n)^4$,输出为$(\beta_0,\beta_1,\beta_2,\beta_3)^{\mathrm{T}}\in(Z_2^n)^4$.

定理 3 对 Z_2^n 上一类特殊的比特变换$(a_0,a_1,a_2,a_3)\xrightarrow{\wedge(c_0,c_1,c_2,c_3)}(b_0,b_1,b_2,b_3)$而言,"1→3"型输入输出对和"3→1"型输入输出对的个数相等,且都为 $4\times\sum_{i=1}^{4}(2^{N_i}-1)$个.

证明 由比特变换的对合性质即知"1→3"型输入输出对和"3→1"型输入输出对的个数相等.

先分析输入形如$(0,0,0,\alpha_3)^{\mathrm{T}}(\alpha_3\neq0)$的"1→3"型输入输出对的个数.设 $\alpha_3=\alpha_{3(n-1)}\alpha_{3(n-2)}\cdots\alpha_{30}\in Z_2^n$.由性质 1、性质 2 以及比特变换的定义,$\alpha_3$ 只能为以下四种情形之一:

(1) $\alpha_{3(N_1-1)}\cdots\alpha_{30}\in Z_2^{N_1}\setminus\{0\}$,
$\alpha_{3j}=0(\forall j,j\neq0,\cdots,N_1-1)$;

(2) $\alpha_{3(N_1+N_2-1)}\cdots\alpha_{3N_1}\in Z_2^{N_2}\setminus\{0\}$,
$\alpha_{3j}=0(\forall j,j\neq N_1,\cdots,N_1+N_2-1)$;

(3) $\alpha_{3(N_1+N_2+N_3-1)}\cdots\alpha_{3(N_1+N_2)}\in Z_2^{N_3}\setminus\{0\}$,
$\alpha_{3j}=0(\forall j,j\neq N_1+N_2,\cdots,N_1+N_2+N_3-1)$;

(4) $\alpha_{3(n-1)}\cdots\alpha_{3(N_1+N_2+N_3)}\in Z_2^{N_4}\setminus\{0\}$,
$\alpha_{3j}=0(\forall j,j\neq N_1+N_2+N_3,\cdots,n-1)$.

从而 α_3 有 $\sum_{i=1}^{4}(2^{N_i}-1)$种取法,故输入形如$(0,0,0,\alpha_3)^{\mathrm{T}}(\alpha_3\neq0)$的"1→3"型输入输出对有 $\sum_{i=1}^{4}(2^{N_i}-1)$个.同理,输入形如$(0,0,\alpha_2,0)^{\mathrm{T}}(\alpha_2\neq0)$、$(0,\alpha_1,0,0)^{\mathrm{T}}(\alpha_1\neq0)$和$(\alpha_0,0,0,0)^{\mathrm{T}}(\alpha_0\neq0)$的"1→3"型输入输出对也各有 $\sum_{i=1}^{4}(2^{N_i}-1)$个,故"1→3"型输入输出对共有 $4\times\sum_{i=1}^{4}(2^{N_i}-1)$个. 证毕

类似地,可以证明定理 4.

定理 4 对 Z_2^n 上一类特殊的比特变换$(a_0,a_1,a_2,a_3)\xrightarrow{\wedge(c_0,c_1,c_2,c_3)}(b_0,b_1,b_2,b_3)$而言,"2→2"型输入输出对的个数为 $4\times\sum_{i=1}^{4}(2^{N_i}-1)+2^{N_1+N_3+1}+2^{N_2+N_4+1}-4$.

定理 5 对 Z_2^n 上一类特殊的比特变换$(a_0,a_1,a_2,a_3)\xrightarrow{\wedge(c_0,c_1,c_2,c_3)}(b_0,b_1,b_2,b_3)$而言,达到最小扩散的输入输出对的个数为 $12\times\sum_{i=1}^{4}(2^{N_i}-1)+2^{N_1+N_3+1}+2^{N_2+N_4+1}-4$.

证明 由定理 3 和定理 4 知,"1→3"型、"3→1"型和"2→2"型输入输出对的总个数为

$$8\times\sum_{i=1}^{4}(2^{N_i}-1)+4\times\sum_{i=1}^{4}(2^{N_i}-1)+2^{N_1+N_3+1}+2^{N_2+N_4+1}-4$$
$$=12\times\sum_{i=1}^{4}(2^{N_i}-1)+2^{N_1+N_3+1}+2^{N_2+N_4+1}-4$$

即本定理结论成立. 证毕

定理 6 对 Z_2^n 上一类特殊的比特变换$(a_0,a_1,a_2,a_3)\xrightarrow{\wedge(c_0,c_1,c_2,c_3)}(b_0,b_1,b_2,b_3)$而言,达到最小扩散的输入输出对的个数占输入输出对总数的比例 $<\frac{7}{2^{2n-2}}$.

证明 只需证明

$$\frac{12\times\sum_{i=1}^{4}(2^{N_i}-1)+2^{N_1+N_3+1}+2^{N_2+N_4+1}-4}{2^n\times2^n\times2^n\times2^n}<\frac{7}{2^{2n-2}}$$

即可. 证毕

定理 6 表明,达到最小扩散的输入输出对的个数占输入输出对总数的比例很小. Crypton[9] 扩散层中的变换 π_0 和 π_1 都是 Z_2^{32} 上一类特殊的比特变换,故达到最小扩散的输入输出对的个数占输入输出对总数的比例 $<\frac{7}{2^{62}}$.

4 结束语

本文对一类特殊的比特变换进行了详细地研究.证明了该类比特变换是 Z_2^n 上的对合变换,且其分支数等于 4.进一步的分析表明,达到最小扩散的输入输出对的个数占输入输出对总数的比例很小.事实上,可以证明 Z_2^n 上基于逐比特逻辑与运算的比特变换的分支数不可能达到最大值 5,从而本文所研究的一类特殊的比特变换具有较好的扩散性.

参考文献

[1] 崔霆,金晨辉.对合 Cauchy-Hadamard 型 MDS 矩阵的构造[J].电子学报,2010,32(2):500 – 503.
Cui Ting, Jin Chen-hui. Construction of Involution Cauchy-Hadamard type MDS matrices[J]. Acta Electronica Sinica, 2010,32(2):500 – 503.(in Chinese)

[2] 王念平,金晨辉,余昭平.对合型列混合变换的研究[J].电子学报,2005,33(10):1917 – 1920.
Wang Nian-ping, Jin Chen-hui, Yu Zhao-ping. Research on involution-typed mixcolumn transform[J]. Acta Electronica Sinica, 2005,33(10):1917 – 1920.(in Chinese)

[3] J Daemen, V Rijmen. The Design of Rijndael: AES – The Advanced Encryption Standard[M]. Springer-verlag, 2002.

[4] B. Schneier, J Kelsey, D Whiting, D Wagner, C Hall, N Ferguson. Twofish: A 128-bit Block Cipher. Primitive submitted to

AES[OL]. Available at http://www.schneier.com/,2007-2-2.

[5] NTT-Nippon Telegraph and Telephone Corporation. E2: Efficient Encryption Algorithm[OL]. Available at http://info.isl.ntt.co.jp/e2,2007-2-2.

[6] K Aoki, T Ichikawa, M Kanda, M Matsui, S Moriai, J Nakajima, T Tokita. Camellia: a 128-bit block cipher suitable for multiple platforms[A]. Proceedings of Selected Areas in Cryptography-SAC'00[C]. LNCS 2012, Springer-Verlag, 2001. 41 – 54.

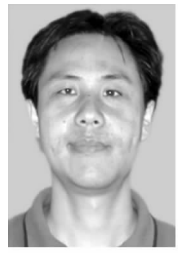
[7] J Massey. SAFER K-64: A byte-oriented block-ciphering algorithm[A]. Proceedings of Fast Software Encryption-FSE'94[C]. LNCS 809, Springer-Verlag, 1994. 1 – 17.

[8] J Massey, G H Khachatrian, M K Kuregian. The SAFER + + Block Encryption Algorithm[OL]. Available at http://cryptonessie.org,2007-1-1.

[9] C H Lim. Crypton: A New 128-bit Block Cipher[OL]. Available at the NIST's AES homepage, URL: http://www.nist.gov/aes,2007-4-1.

[10] 冯国柱,李超,多磊,谢端强,戴清平. 变型的 Rijndael 及其差分和统计特性[J]. 电子学报,2002,30(10):1544 – 1546.
Feng Guo-zhu, Li Chao, Duo Lei, Xie Duan-qiang, Dai Qing-ping. Transmutative Rijndael with the differential and statistical characteristics[J]. Acta Electronica Sinica, 2002, 30(10): 1544 – 1546. (in Chinese)

作者简介



王念平　男,1973 年 6 月出生于河南洛阳,博士,副教授,硕士生导师. 主要研究方向为信息安全、密码学.
E-mail: wwnnpp@126.com