基于循环移位和异或运算的对合线性变换研究*

李瑞林,熊 海,李 超
(国防科技大学 理学院,湖南 长沙 410073)

摘 要:在对称密码算法的设计中,为达到良好的扩散作用,设计者一般均选择分支数较大的线性变换。基于循环移位和异或运算的线性变换由于其实现效率较高,已经在很多密码算法中被采用,比如分组密码SMS4、HIGHT,Hash函数SHA-2、MD6等。此外,如果线性变换是对合的,还为解密带来了方便。研究了基于循环移位和异或运算设计的对合线性变换,给出了这类线性变换的计数公式,指出它们的分支数上界为4,并讨论了循环移位的参数与分支数之间的关系,从而为基于这类运算设计的线性变换提供了理论依据。

关键词:对称密码;线性变换;分支数;循环移位;异或
中图分类号:TN918 **文献标志码**:A **文章编号**:1001-2486(2012)02-0046-05

Research on involutional linear transformations based on rotation and XOR

LI Ruilin, *XIONG Hai*, *LI Chao*
(College of Science, National University of Defense Technology, Changsha 410073, China)

Abstract: Linear transformation with good branch number plays a significant role in designing components of symmetric key primitives. Linear transformation based on XOR of several rotations can be efficiently implemented, and has been widely used in the block ciphers such as SMS4, HIGHT and the hash functions SHA-2, MD6. Besides, if the linear transformation is involutional, it will facilitate the decryption process. In view of this, a kind of involutional linear transformation based on the XOR of several rotations was studied, the numeration of this kind of linear transformation was given and the branch number was shown to be upper bounded by 4. Meanwhile, the relationship between the parameters of the rotations and the branch number was discussed, which provides a theoretical basis for the design.

Key words: symmetric key cryptography; linear transformation; branch number; rotation; XOR

分支数的概念首先在文献[1]中提出,它是度量连续两轮SPN结构活跃S盒数目下界的一个重要指标。很多分组密码算法均采用分支数达到最大时的线性变换来提供良好的扩散性能。因此,研究分支数最优时线性变换的构造方法[2-3]具有重要的意义。

基于循环移位和异或运算设计的线性变换,由于其实现效率较高,已被很多对称密码算法所采用,比如分组密码SMS4、HIGHT,Hash函数SHA-2、MD6等。此外,如果线性变换是对合的,则还为解密带来了方便。文献[4]研究了基于循环移位和异或运算设计的线性变换分支数达到最优时需要满足的一些必要条件,文献[5]研究了SMS4-型的线性变换,指出在一定的等价意义下,这样的最优线性变换仅有2个。

1 预备知识

本节给出了相关的预备知识。

定义1 给定$\mathbb{F}_2^{mn}\to\mathbb{F}_2^{mn}$的线性变换$L$,称$L$仅由循环移位和异或运算构成,是指$L$可通过如下表达式生成

$$L(X)=\bigoplus_{i=1}^{k}(X\lll r_i)$$

其中,$0\leqslant r_1<r_2<\cdots<r_k\leqslant mn-1$,$k\leqslant mn$。

定义2 给定$X\in\mathbb{F}_2^{mn}$,以m比特为单位可将X划分为n个分量,即

$$X=(X_1,X_2,\cdots,X_n)$$

其中$X_i\in\mathbb{F}_2^m$,令$H_w(X)=\#\{i\mid X_i\neq 0\}$表示$X$中非零分量的个数,则称$H_w(X)$为$X$针对分块$\mathbb{F}_2^m$的字重量,简称$H_w(X)$为$X$的重量。

* **收稿日期**:2011-07-28
基金项目:国家自然科学基金资助项目(61070215,61103192);信息安全国家重点实验室开放基金资助项目(01-02-5)
作者简介:李瑞林(1982—),男,山西太原人,博士研究生,E-mail:securitylrl@163.com;
李超(通信作者),男,教授,博士,博士生导师,E-mail:lichao_nudt@sina.com

定义 3　线性变换 L 的分支数定义为

$$\mathscr{B}(L)=\min_{X\neq 0}(H_w(X)+H_w(L(X)))$$

由定义 1 和定义 3 知,任给线性变换 L,$\mathscr{B}(L)\leqslant n+1$,称分支数达到最大的变换为最优变换。比如,SMS4 算法[6]扩散层的线性变换定义为 $\mathbb{F}_2^{32}$ 上的线性变换 L,其中 $m=8,n=4,L=X\oplus(X\lll 2)\oplus(X\lll 10)\oplus(X\lll 18)\oplus(X\lll 24)$,而 $\mathscr{B}(L)=5$。

2　对合线性变换的计数

本节给出基于循环移位和异或运算设计的对合线性变换的具体表达式和计数公式,首先给出如下引理。

引理 1　如果 $\mathbb{F}_2^{mn}$ 上仅由循环移位和异或运算构成的线性变换 $L(X)=\bigoplus_{i=1}^{k}(X\lll r_i)$ 可逆,则 k 为奇数。

证明　考虑剩余类环 $\mathbb{F}_2[x]/(x^{mn}\oplus 1)$。假设输入 $B=(B_{mn-1},B_{mn-2},\cdots,B_1,B_0)\in\mathbb{F}_2^{mn}$,则可以建立 $\mathbb{F}_2^{mn}$ 中元素 B 与剩余类环中元 $B(x)=B_0\oplus B_1x\oplus\cdots\oplus B_{mn-2}x^{mn-2}\oplus B_{mn-1}x^{mn-1}$ 的一一对应关系,而 $B\lll i$,可等价刻画为 $B(x)\cdot x^i\pmod{(x^{mn}\oplus 1)}$。

令 $l(x)=x^{r_1}\oplus x^{r_2}\oplus\cdots\oplus x^{r_k}$,则

$$\begin{array}{ccc} L:\mathbb{F}_2^{mn}\to\mathbb{F}_2^{mn} & \Leftrightarrow & \mathscr{L}:\mathbb{F}_2[x]/(x^{mn}\oplus 1)\to\mathbb{F}_2[x]/(x^{mn}\oplus 1)\\ \updownarrow & & \updownarrow\\ B\mapsto L(B) & \Leftrightarrow & B(x)\mapsto\mathscr{L}(B(x))=B(x)\cdot l(x)\pmod{(x^{mn}\oplus 1)} \end{array}$$

注意到 $1\oplus x\mid 1\oplus x^{mn}$,故若 k 为偶数,则 $1\oplus x\mid l(x)$,因此 $\gcd(l(x),x^{mn}\oplus 1)\neq 1$. 这表明在剩余类环 $\mathbb{F}_2[x]/(x^{mn}\oplus 1)$ 中,$\mathscr{L}$ 变换不可逆,因此 L 在 $\mathbb{F}_2^{mn}$ 中也不可逆,与引理中的条件矛盾。故 k 为奇数。

引理 1 表明,$\mathbb{F}_2^{mn}$ 上基于循环移位和异或运算设计的线性变换可逆时,对应表达式中循环移位的个数必须为奇数。下面的定理则进一步给出了当这类线性变换对合时,对应的循环移位参数需要满足的关系。

定理 1　当 mn 为奇数时,$\mathbb{F}_2^{mn}$ 上基于循环移位和异或运算的对合线性变换只有 1 个,即恒等变换。当 mn 为偶数时,$\mathbb{F}_2^{mn}$ 上基于循环移位和异或运算的对合线性变换共有 $2^{mn/2}$ 个,且循环移位参数 $\{r_1,r_2,\cdots,r_k\}$ 满足如下关系之一:

(1) $r_1=0$, $r_{i+(k-1)/2}=r_i+\dfrac{mn}{2}$, $i=2,3,\cdots,\dfrac{k+1}{2}$

(2) $r_{(k+1)/2}=mn/2$, $r_{i+(k-1)/2}=r_i+\dfrac{mn}{2}$, $i=1,2,\cdots,\dfrac{k-1}{2}$

证明　考虑剩余类环 $\mathbb{F}_2[x]/(x^{mn}\oplus 1)$,则 L 是 $\mathbb{F}_2^{mn}$ 上的对合线性变换,当且仅当 $\mathscr{L}$ 是 $\mathbb{F}_2[x]/(x^{mn}\oplus 1)$ 中的对合变换,即

$$l^2(x)\equiv 1\pmod{x^{mn}\oplus 1}$$

注意到 $l(x)=x^{r_1}\oplus x^{r_2}\oplus\cdots\oplus x^{r_k}$,因此

$$x^{2r_1}\oplus x^{2r_2}\oplus\cdots\oplus x^{2r_k}\equiv 1\pmod{x^{mn}\oplus 1}\quad(1)$$

令

$$\begin{cases} 2r_1\equiv t_1\pmod{mn}\\ 2r_2\equiv t_2\pmod{mn}\\ \quad\vdots\\ 2r_k\equiv t_k\pmod{mn}\end{cases}$$

其中 $0\leqslant t_i\leqslant mn-1$。此时(1)式转化为

$$x^{t_1}\oplus x^{t_2}\oplus\cdots\oplus x^{t_k}=1\quad(2)$$

(1)当 mn 为奇数时,$\gcd(2,mn)=1$,故 t_i 必须两两不同。否则存在 $i\neq j$,使得 $t_i=t_j$,从而 $2r_i\equiv 2r_j\pmod{mn}$,由此得 $r_i=r_j$,矛盾。此时,(2)式表明,$k=1$,且 $t_1=0$,即 $l(x)=1$,从而 L 为恒等变换。

(2)当 mn 为偶数时,(2)式表明,仅存在某个 $i\in\{1,2,\cdots,k\}$,使得 $t_i=0$,且其余 $j\in\{1,2,\cdots,k\}$,$j\neq i$,必须两两匹配满足 $t_{j_1}=t_{j_2}$,否则假设存在某个 t_{j_3},满足 $t_{j_3}=t_{j_2}=t_{j_1}$,不妨设对应的 $r_{j_1}<r_{j_2}<r_{j_3}$,注意到 $2r_j\equiv t_j\pmod{mn}$,从而有

$$2r_{j_1}\equiv 2r_{j_2}\equiv 2r_{j_3}\pmod{mn}$$

故

$$r_{j_1}\equiv r_{j_2}\equiv r_{j_3}\pmod{mn/2}$$

由 $0<r_{j_2}-r_{j_1}<mn-1$,从而有

$$\begin{cases} r_{j_2}-r_{j_1}=mn/2\\ r_{j_3}-r_{j_1}=mn/2\end{cases}$$

故 $r_{j_3}=r_{j_2}$,矛盾。

由 $t_i=0$,得 $r_i=0$ 或 $r_i=mn/2$,因此有 $r_1=0$ 或者 $r_{(k+1)/2}=mn/2$。

1)当 $r_1=0$ 时,对 $j\in\{2,3,\cdots,(k+1)/2\}$,有 $r_{j+(k-1)/2}=r_j+mn/2$;

2)当 $r_{(k+1)/2}=mn/2$ 时,对 $j\in\{1,2,\cdots,(k-1)/2\}$,有 $r_{j+(k-1)/2}=r_j+mn/2$。

这表明,对于循环移位参数 $\{r_1, r_2, \cdots, r_k\}$ 而言,$r_1 = 0$ 或者 $r_{(k+1)/2} = mn/2$,其余 $k-1$ 个参数中,如果前面 $(k-1)/2$ 个参数确定,则后面 $(k-1)/2$ 个参数亦唯一确定。

注意到前面 $(k-1)/2$ 个参数的取值范围为

$$\{1, 2, \cdots, (mn/2)-1\},$$

故当 mn 为偶数时,这类对合线性变换的数目为

$$2 \times \sum_{k=1, k\text{为奇数}}^{mn-1} \binom{(mn/2)-1}{(k-1)/2} = 2 \times 2^{(mn/2)-1} = 2^{mn/2}$$

3 对合线性变换的分支数研究

本节讨论 $\mathbb{F}_2^{mn}$ 上仅由循环移位和异或运算构成的对合线性变换 L 的分支数,注意到当 mn 为奇数时,L 为恒等变换,此时 $\mathscr{B}(L) = 2$,故本节只讨论 mn 为偶数时的情形。

定理 2 设 L 为 $\mathbb{F}_2^{mn}$ 上仅由循环移位和异或运算构成的对合线性变换,当 mn 为偶数时,有 $\mathscr{B}(L) \leqslant 4$。

证明 根据定理 1 的结论,当 mn 为偶数时,不妨设(另一种证明情形下的证明过程类似)线性变换 $L(X) = \bigoplus_{i=1}^{k} (X \lll r_i)$ 的循环移位参数 $\{r_1, r_2, \cdots, r_k\}$ 满足

$$r_1 = 0$$

$$r_{i+(k-1)/2} = r_i + (mn/2), i = 2, 3, \cdots, (k+1)/2$$

当 $n \leqslant 3$ 时,结论显然成立,故只需考虑 $n \geqslant 4$ 时的情形,选取特殊的输入

$$X = (x_{mn-1}, x_{mn-2}, \cdots, x_2, x_1, x_0)$$

满足

$$\begin{cases} x_i = 1, i = mn - r_2, mn - r_2 - mn/2 \\ x_i = 0, \text{其他} \end{cases}$$

容易验证 $H_w(X) = 2$,且 $H_w(L(X)) = 2$,因此,$\mathscr{B}(L) \leqslant 4$。

定理 2 表明基于循环移位和异或运算构成的对合线性变换 L 的分支数不超过 4,下面将进一步研究满足什么条件的对合线性变换其分支数可以达到 4。

注意到 $\mathbb{F}_2^{mn}$ 可视为 $\mathbb{F}_2$ 上的 mn 维线性空间,因此取其中的一组基如下:

$$\begin{cases} \varepsilon_1 = (1, 0, 0, \cdots, 0) \\ \varepsilon_2 = (0, 1, 0, \cdots, 0) \\ \varepsilon_3 = (0, 0, 1, \cdots, 0) \\ \quad \vdots \\ \varepsilon_{mn} = (0, 0, 0, \cdots, 1) \end{cases}$$

则线性变换 $L(X) = \bigoplus_{i=1}^{k} (X \lll r_i)$ 在上述基下可以表示为 $\mathbb{F}_2$ 上的 $mn \times mn$ 的矩阵 M,进一步可以将 M 视为如下的 $n \times n$ 的分块矩阵

$$M = \begin{bmatrix} M_{1,1} & M_{1,2} & \cdots & M_{1,n} \\ M_{2,1} & M_{2,2} & \cdots & M_{2,n} \\ \vdots & \vdots & \vdots & \vdots \\ M_{n,1} & M_{n,2} & \cdots & M_{n,n} \end{bmatrix},$$

其中 $M_{i,j} \in \mathbb{F}_2^{m \times m}$。

下面的引理表明,分块矩阵 M 实际上是循环矩阵,即矩阵 M 可由第一行循环右移生成。注意到,本节所采用的模 n 剩余系是指 $\{1, 2, \cdots, n\}$,模 $n/2$ 剩余系是指 $\{1, 2, \cdots, n/2\}$(当 n 为偶数时)。

引理 2 线性变换 $L(X) = \bigoplus_{s=1}^{k} (X \lll r_s)$ 对应的矩阵 M 是循环矩阵,即

$$M_{i,j} = M_{1,(j-i+1) \bmod n}$$

证明 考虑变换 $L_s(X) = X \lll r_s$,容易证明 L_s 对应的矩阵表示 $M^{(s)}$ 是循环矩阵,即

$$M_{i,j}^{(s)} = M_{i,(j-i+1) \bmod n}^{(s)}$$

注意到 $M = \bigoplus_{s=1}^{k} M^{(s)}$,故

$$M_{i,j} = \bigoplus_{s=1}^{k} M_{i,j}^{(s)} = \bigoplus_{s=1}^{k} M_{i,(j-i+1) \bmod n}^{(s)} = M_{i,(j-i+1) \bmod n}$$

因此,L 对应的矩阵 M 是循环矩阵。

为方便起见,将矩阵 M 的第一行简记为 $M_1, M_2, M_3, \cdots, M_n$,并将循环矩阵 M 简记为 $M = Circ(M_1, M_2, \cdots, M_n)$。

实际当中,一般将 n 设计为偶数,而 m 没有限制(一般 $m \geqslant 3$ 即可)。下面我们给出当 n 为偶数时,如何选取循环移位参数使得该对合线性变换的分支数达到 4。

首先给出如下引理:

引理 3 如果 $\mathbb{F}_2^{mn}$ 上的线性变换 $L(X) = \bigoplus_{s=1}^{k} (X \lll r_s)$ 对合,则当 n 为偶数时,存在 $m \times m$ 的矩阵 $A_1, A_2, \cdots, A_{n/2}$,使得 L 对应的循环矩阵 $M = Circ(M_1, M_2, \cdots, M_n)$ 满足如下关系:

$$M_1 = A_1, M_{n/2+1} = A_1 \oplus E,$$

$$M_i = M_{i+n/2} = A_i, 2 \leqslant i \leqslant n/2$$

其中,E 是 $m \times m$ 的单位矩阵。

证明 因为 L 是对合线性变换,根据定理 1,不妨(另一种情形下的证明类似)设 $r_1 = 0$,$r_{i+(k-1)/2} = r_i + nm/2, 2 \leqslant i \leqslant 1 + (k+1)/2$。

令 $L_1(X) = X \lll 0$,则其对应的循环矩阵为 $Circ(E, 0, \cdots, 0)$,其中 0 表示 $m \times m$ 的全零矩阵。

令 $L_2(X)=\bigoplus_{s=2}^{(k+1)/2+1}(X\lll r_s)$,设其对应的循环矩阵为 $Circ(N_1,N_2,\cdots,N_n)$。

令

$$L_3(X)=(\bigoplus_{s=2}^{(k+1)/2+1}(X\lll r_s))\lll mn/2,$$

则其对应的循环矩阵为

$$Circ(N_{n/2},\cdots,N_n,N_1,\cdots,N_{n/2-1})$$

注意到

$$L(X)=L_1(X)\oplus L_2(X)\oplus L_3(X)$$

故

$$M=Circ(E\oplus N_1\oplus N_{n/2},N_2\oplus N_{n/2+1},\cdots,N_{n/2}\oplus N_1,\cdots,N_n\oplus N_{n/2-1})$$

令 $A_1=E\oplus N_1\oplus N_{n/2}$,$A_i=N_i\oplus N_{i-1+n/2}$,$2\leqslant i\leqslant n/2$,可知引理成立。

引理 3 表明,当 n 为偶数时,对合线性变换 L 对应的矩阵 M 可以由 $A_1,A_2,\cdots,A_{n/2}$ 和单位矩阵 E 完全刻画,我们称 $A_1,A_2,\cdots,A_{n/2}$ 为 M 的约化表示,基于此,有如下结论成立。

定理 3　设 $n\geqslant 4$ 为偶数,$\mathbb{F}_2^{mn}$ 上对合线性变换 $L(X)=\bigoplus_{s=1}^{k}(X\lll r_s)$ 相应矩阵的约化表示为 $A_1,A_2,\cdots,A_{n/2}$,如果存在某个 $2\leqslant l\leqslant n/2$,使得 $\mathrm{rank}(A_l)=m$,则 $\mathscr{B}(L)=4$。

证明　不失一般性,假设 $\mathrm{rank}(A_2)\neq 0$。

下面仅需证明:

当 $H_\omega(X)=1$ 时,$H_\omega(L(X))\geqslant 3$;

当 $H_\omega(X)=2$ 时,$H_\omega(L(X))\geqslant 2$;且存在 X 使得 $H_\omega(X)+H_\omega(L(X))=4$。

若 $H_\omega(X)=1$,不妨设

$$X=(0,\cdots,X_j,\cdots,0)$$

其中 X 的第 j 个分量 $X_j\neq 0$。由于 $\mathrm{rank}(A_2)=m$,因此 $A_2X_j\neq 0$。由引理 3 知,L 对应循环矩阵的第 j 列出现两次 A_2,而注意到 A_1X_j 与 $(A_1\oplus E)X_j$ 不能同时为 0,因此

$$H_\omega(L(X))\geqslant 3$$

若 $H_\omega(X)=2$,不妨设

$$X=(0,\cdots,X_i,\cdots,X_j,\cdots,0)$$

其中 $X_i\neq 0$,$X_j\neq 0$。

(1)若 $j-i=n/2$,则 $L(X)$ 的第 i 个分量为 $A_1X_i\oplus(A_1\oplus E)X_j$,第 j 个分量为 $(A_1\oplus E)X_i\oplus A_1X_j$,第 $(i-1)$ 个分量为 $A_2X_i\oplus A_2X_j$。注意到 A_2 可逆,则上述 3 个分量中至少有两个非零,故 $H_\omega(L(X))\geqslant 2$。

而当 $X_i=X_j$ 时,$L(X)$ 只有第 i 和第 j 个分量非 0,此时 $H_\omega(L(X))=2$,因此 $H_\omega(X)+H_\omega(L(X))=4$。

(2)若 $j-i\neq n/2$,则 $L(X)$ 的第 i 个和第 $(i+(n/2))\bmod n$ 个分量分别为

$$A_1X_i\oplus A_{(1+j-i)\bmod(n/2)}X_j$$

与

$$(A_1\oplus E)X_i\oplus A_{(1+j-i)\bmod(n/2)}X_j$$

故这两个分量中必有一个非零。

而 $L(X)$ 的第 j 个和第 $(j+(n/2))\bmod n$ 个分量分别为

$$A_{(n+1-(j-i))\bmod(n/2)}X_i\oplus A_1X_j$$

与

$$A_{(n+1-(j-i))\bmod(n/2)}X_i\oplus(A_1\oplus E)X_j$$

故这两个分量中也必有一个非零,此时

$$H_\omega(L(X))\geqslant 2$$

根据上述讨论,知定理成立。

4　例　子

根据第 3 节定理 3,本节给出几个分支数达到 4 时的对合线性变换:

$$L(X)=\bigoplus_{i=1}^{k}(X\lll r_i)$$

的具体表达式。当给定 m,n,k 时,只需确定循环移位参数 $\{r_1,r_2,\cdots,r_k\}$ 的取值。注意到这类线性变换的分支数上界为 4,因此在实际设计当中,n 不宜过大,否则扩散性不佳。表 1 列出了当 $n=4$ 时对应的 10 组数据。注意到 $r_1=0$ 和 $r_1=mn/2$ 时对应线性变换的分支数均相同,故表中只列出了当 $r_1=0$ 时对应线性变换的循环移位参数取值。

5　讨　论

本文研究了基于循环移位和异或运算设计的对合线性变换的性质,给出了这类线性变换的计数公式,指出它们的分支数上界为 4,并讨论了循环移位的参数与分支数之间的关系,从而为基于这类运算设计的线性变换提供了理论依据。进一步,将继续研究如何选取循环移位的参数,使得相应线性变换(不一定对合)的分支数达到最大。

参考文献(References)

[1] Daemen J. Cipher and hash function design strategies based on linear and differential cryptanalysis [D]. K. U. Leuven, 1995.

[2] Lu X, Heys H M. Hardware design and analysis of block cipher components [C]// Proc of ICISC 2002, LNCS 2587, Springer, 2003: 164 - 181.

[3] Pascal J, Serge V. Perfect diffusion primitives for block ciphers building efficient MDS matrices [C]// Proc of SAC 2004, LNCS 3357, Springer, 2005: 84 - 99.

表 1 几类分支数为 4 的对合线性变换对应循环移位参数的取值

Tab. 1 Rotation parameters for several involutional linear transformations with branch number 4

m	n	k	循环移位参数
4	4	3	{0 4 12}
4	4	5	{0 1 4 9 12} {0 1 5 9 13} {0 2 4 10 12} {0 2 6 10 14} {0 3 4 11 12} {0 3 5 11 13} {0 3 7 11 15} {0 4 5 12 13} {0 4 6 12 14} {0 4 7 12 15}
8	4	3	{0 8 24}
8	4	5	{0 1 8 17 24} {0 1 9 17 25} {0 2 8 18 24} {0 2 10 18 26} {0 3 8 19 24} {0 3 11 19 27} {0 4 8 20 24} {0 4 12 20 28} {0 5 8 21 24} {0 5 9 21 25} {0 5 13 21 29} {0 6 8 22 24} {0 6 10 22 26} {0 6 14 22 30} {0 7 8 23 24} {0 7 9 23 25} {0 7 11 23 27} {0 7 15 23 31} {0 8 9 24 25} {0 8 10 24 26} {0 8 11 24 27} {0 8 12 24 28} {0 8 13 24 29} {0 8 14 24 30} {0 8 15 24 31}
3	4	3	{0 3 9}
3	4	5	{0 1 3 7 9} {0 1 4 7 10} {0 2 3 8 9} {0 2 5 8 11} {0 3 4 9 10} {0 3 5 9 11}
5	4	3	{0,5,15}
5	4	5	{ 0 1 5 11 15} { 0 1 6 11 16} { 0 2 5 12 15} { 0 2 7 12 17} { 0 3 5 13 15} { 0 3 8 13 18} { 0 4 5 14 15} { 0 4 9 14 19} { 0 5 6 15 16} { 0 5 7 15 17} { 0 5 8 15 18} { 0 5 9 15 19
7	4	3	{0,7,21}
7	4	5	{0 1 7 15 21} {0 1 8 15 22} {0 2 7 16 21} {0 2 9 16 23} {0 3 7 17 21} {0 3 10 17 24} {0 4 7 18 21} {0 4 11 18 25} {0 5 7 19 21} {0 5 12 19 26} {0 6 7 20 21} {0 6 13 20 27} {0 7 8 21 22} {0 7 9 21 23} {0 7 10 21 24} {0 7 11 21 25} {0 7 12 21 26} {0 7 13 21 27}

[4] Zhang W T, Wu W L, Feng D G, et al. Some new observations on the SMS4 block cipher in the Chinese WAPI standard [C]// Proc of ISPEC 2009, LNCS 5451, Springer, 2009: 324 – 335.

[5] 王金波. 基于循环移位构造最优线性变换 [C]//中国密码学会 2007 年会论文集, 2007: 306 – 307.
WANG Jinbo. The optimal permutation in cryptography based on cyclic-shift linear transform [C]// Proc of Chinacrypt 2007, 2007: 306 – 307. (in Chinese)

[6] 国家商用密码管理办公室. 无线局域网产品使用的 SMS4 密码算法[EB/OL]. [2011 – 06 – 15]. http://www.oscca.gov.cn/UpFile/200622026423297990.pdf.
Office of state commercial cipher administration. Block cipher for WLAN products-SMS4 [EB/OL]. [2011 – 06 – 15]. http://www.oscca.gov.cn/UpFile/200622026423297990.pdf. (in Chinese)