文章编号:1009-3087(2013)06-0001-07

正形置换的一些新结论

童 言[1],张焕国[2,3],池志强[1],黄治华[1],张 剑[1]
(1. 武汉数字工程研究所,湖北 武汉 430074;2. 武汉大学 计算机学院,湖北 武汉 430072;
3. 武汉大学 空天信息安全与可信计算教育部重点实验室,湖北 武汉 430072)

摘 要:正形置换在对称密码的设计中占有重要的地位。为了对正形置换的构造计数和性质进行进一步的分析探讨,首先指出戴宗铎等关于线性正形置换结构的结论中存在的问题,并根据修改后的结论,得到了最大线性正形置换的结构形式,进而实现了最大线性正形置换的完全无重复构造,而原先的构造方法会产生重复的结果;通过分析正形置换的补置换和仿射正形置换的关系,得到了正形置换的个数为2的($n+1$)次方的倍数,比原来为2的n次方的倍数的结论更进了一步;给出了一种代数免疫度的定义,证明了这样定义的代数免疫度是Carlet-Charpin-Zinoviev等价不变量,并得到非仿射正形置换与它的补置换的差分均匀度、非线性度、代数次数和代数免疫度均相等。

关键词:对称密码;正形置换;最大线性正形置换;代数免疫度;CCZ等价
中图分类号:TP309 **文献标志码**:A

Some New Conclusions on Orthomorphisms

TONG Yan[1], *ZHANG Huan-guo*[2,3], *CHI Zhi-qiang*[1], *HUANG Zhi-hua*[1], *ZHANG Jian*[1]
(1. Wuhan Digital Eng. Inst., Wuhan 430074, China; 2. School of Computer, Wuhan Univ., Wuhan 430072, China;
3. Key Lab. of Aerospace Info. Security and Trusted Computing of Ministry of Education, Wuhan Univ., Wuhan 430072, China)

Abstract: Orthomorphism plays an important role in the design of symmetric cryptography. To analyze its construction, counting and properties further, a problem in a conclusion about linear orthomorphism was pointed out and corrected. Then, with the corrected conclusion, a non-redundant construction method to generate all maximal linear orthomorphisms was presented, while the previous method would produce repeatable results. The number of orthomorphism was proved to be a multiple of 2 to the power $(n+1)$ based on the relationship between affine orthomorphism and complementary permutation. At last, a definition of algebraic immunity was proposed and proved to be CCZ-equivalence-invariant. The algebraic immunity of a non-affine orthomorphism was also proved to be equal to that of complementary permutation of this orthomorphism. Same is the case with some other cryptographic properties, such as difference uniformity, nonlinearity and algebraic degree.

Key words: symmetric cryptography; orthomorphism; orthomorphic permutation; linear orthomorphism; algebraic immunity; CCZ-equivalence

正形置换是密码学中一类基础的置换。1995年,美国Teledyne电子技术公司(TET)的Mittenthal博士,首次公开的将正形置换的理论用于密码算法的设计中[1]。正形置换具有完全平衡性等优良的密码学性质,可用于构造对称密码中的S盒[2-3]。中国无线局域网中的商用密码算法SMS4[4]的轮函数,也是基于BDLL正形置换发生器设计的[5]。

国内外的许多学者对于正形置换的构造和计数进行了大量的研究[1,6-8]。线性正形置换的研究较早展开,但是关于线性正形置换的无重复构造的结论[9]中存在问题。而且目前公开发表的文献,对于正形置换的密码学性质的关注还显得不是很充分,数量不多[2-3,10]。

作者首先指出文献[9]给出的关于线性正形置换结构的结论中存在的问题,接着基于修改后的结

收稿日期:2013-06-15
基金项目:国家自然科学基金资助项目(60673071;60970115;61003267;91018008;61003268);国防预研项目(B0820132036;10113011010201)
作者简介:童 言(1982—),男,工程师,博士. 研究方向:密码学;信息安全. E-mail: tongyan.cherish@139.com

论,给出了完全无重复构造最大线性正形置换的方法,而原先的方法会重复构造[11];然后证明了 F_2^n 上的正形置换个数为 2^{n+1} 的倍数,相比原来为 2^n 的倍数的结论[5],实现了更进一步;最后给出了一种代数免疫度的定义,证明了该定义是 CCZ 等价不变量,并证明了非仿射正形置换和它的补置换具有相等的差分均匀度、非线性度、代数次数和代数免疫度。

1 预备知识

用到的主要数学符号如下,如无特殊说明均以此为准:

F_q^n:有限域 $GF(q)$ 上的 n 维向量空间,也就是 $GF(q)^n$;

$\oplus$:表示二进制位按位模二加;

$|A|$:如果 A 为集合,则该符号表示集合 A 内元素的个数,也就是集合的势,比如 $|\{1,2,3\}|=3$;如果 A 为数值,则该符号表示 A 的绝对值;

$\cdot$:向量的内积运算符,比如

$$\boldsymbol{x}=(x_1,x_2,\cdots,x_n),\ \boldsymbol{y}=(y_1,y_2,\cdots,y_n),$$
$$\boldsymbol{x}\cdot\boldsymbol{y}=x_1y_1\oplus x_2y_2\oplus\cdots\oplus x_ny_n;$$

假设 $\boldsymbol{a}\in F_2^n$, $\boldsymbol{a}=(a_0,a_1,\cdots,a_{n-1})$, $a_i\in F_2$, $0\le i<n$。若取 $b=\sum_{i=0}^{n-1}a_i2^i$,则 $\varphi:\boldsymbol{a}\to b$ 是 F_2^n 到 Z_{2^n} 上的同构映射,在之后的讨论中,视 $\boldsymbol{a}$ 与 b 等价。

定义 1[1] 设 σ 是 F_2^n 上的置换,

$$S(\boldsymbol{x})=\sigma(\boldsymbol{x})\oplus\boldsymbol{x},$$

如果 S 也是 F_2^n 上的置换,则称 σ 是 F_2^n 上的正形置换。同时 S 称为 σ 的补置换。

计 F_2^n 上全体正形置换的集合为 $O_n(F_2)$。

假设 $\sigma\in O_n(F_2)$,

$$\sigma=\begin{pmatrix}0 & 1 & \cdots & 2^n-1\\ x_0 & x_1 & \cdots & x_{2^n-1}\end{pmatrix},$$

其中,$\sigma(i)=x_i$, $0\le i<n$。σ 可以简单标识为 $\sigma=(x_0,x_1,\cdots,x_{2^n-1})$。

定义 2[1] F_2^n 上的置换 σ 为正形置换,如果 σ 同时也为线性变换,则称 σ 为 F_2^n 上的线性正形置换。

计 F_2^n 上全体线性正形置换的集合为 $LO_n(F_2)$。

定义 3[1] 如果 $\sigma\in O_n(F_2)$,并且 σ 的圈结构为:

$$\sigma=(x_{i_0})(x_{i_1},x_{i_2},\cdots,x_{i_{2^n-1}}),$$

其中,$i_j(0\le j<2^n)$ 为 $0,1,2,\cdots,2^n-1$ 的一个排列,则称 σ 为 F_2^n 上的最大正形置换。

计其中的全体最大线性正形置换的集合为 $MLO_n(F_2)$。

定义 4[12] Boolean 函数 $f:F_2^n\to F_2$ 的非线性度 $N(f)$ 定义为 f 与所有仿射函数的最小距离,即

$$N(f)=\min_{l\in L_w[x]}d_{\mathrm{H}}(f,l),$$

其中,$L_w[x]$ 表示所有 n 元线性和仿射函数组成的集合,$d_{\mathrm{H}}(f,l)$ 表示 f 和 l 的 Hamming 距离。

定义 5[12] 设 $n\times m$ 多输出函数

$$A(\boldsymbol{x})=(A_0(\boldsymbol{x}),\cdots,A_{m-1}(\boldsymbol{x})),$$

其中,$\boldsymbol{x}=(x_0,\cdots,x_{n-1})\in F_2^n$, A_i 为 $F_2^n\to F_2$ 上的 Boolean 函数,则定义 A 的非线性度为:

$$N(A)=\min\{N(\boldsymbol{\beta}\cdot A)\mid\boldsymbol{\beta}\in F_2^m,\boldsymbol{\beta}\ne0\}=$$
$$\min\{N(\bigoplus_{i=1}^{m}\beta_iA_i(\boldsymbol{x}))\mid(\beta_0,\cdots,\beta_{m-1})\in F_2^m,$$
$$(\beta_0,\cdots,\beta_{m-1})\ne0\}=2^{n-1}-2^{-1}\max_{\boldsymbol{\beta}\in F_2^n,\boldsymbol{\beta}\ne0}\max_{\boldsymbol{\omega}\in F_2^n}|S_{(\boldsymbol{\beta},A)}(\boldsymbol{\omega})|,$$

其中,$S_f(\boldsymbol{\omega})=\sum_{x=0}^{2^n-1}(-1)^{\boldsymbol{\omega}\cdot x\oplus f(x)}$ 表示布尔函数 f 的循环 Walsh 谱。多输出函数的非线性度越高,则它抗击线性密码分析的能力就越强。

定义 6[12] 设 $n\times m$ 多输出函数

$$A(\boldsymbol{x})=(A_0(\boldsymbol{x}),\cdots,A_{m-1}(\boldsymbol{x})),$$
$$\boldsymbol{x}=(x_0,\cdots,x_{n-1})\in F_2^n,$$

定义

$$D(A)=\min\{\deg(\bigoplus_{i=0}^{m-1}b_iA_i(\boldsymbol{x}))\mid(b_0,\cdots,b_{m-1})\in F_2^m,$$
$$(b_0,\cdots,b_{m-1})\ne0\}$$

为 A 的代数次数。其中,$\deg(\cdot)$ 表示布尔函数的代数次数。多输出函数的代数次数越高,则抗击利用较低次布尔函数快速逼近的能力就越强。

定义 7[12] 设 $n\times m$ 多输出函数

$$A(\boldsymbol{x})=(A_0(\boldsymbol{x}),\cdots,A_{m-1}(\boldsymbol{x})),$$
$$\boldsymbol{x}=(x_0,\cdots,x_{n-1})\in F_2^n,$$

定义

$$\tau(A)=\max_{\boldsymbol{\alpha}\in F_2^n,\boldsymbol{\alpha}\ne0,\boldsymbol{\beta}\in F_2^m}|\{\boldsymbol{x}\in F_2^n\mid A(\boldsymbol{x})\oplus A(\boldsymbol{x}\oplus\boldsymbol{\alpha})=\boldsymbol{\beta}\}|$$

为 A 的差分均匀度。多输出函数的差分均匀度越低,则它抗击差分密码分析的能力就越强。

定义 8[13] 如果 S 为 $F_2^n\to F_2^n$ 的映射,A_1 和 A_2 为 F_2^n 上的仿射置换,则称 $A_1\circ S\circ A_2$ 和 S 仿射等价;如果 A_3 为 $F_2^n\to F_2^n$ 的仿射映射,则称 $A_1\circ S\circ A_2+A_3$ 和 S 扩展仿射(EA)等价,简称 EA 等价。

定义 9[13] 如果 S 和 S' 都为 $F_2^n\to F_2^n$ 的映射,并且定义 S 和 S' 的图像分别为:

$$G_S = \{(\boldsymbol{x}, S(\boldsymbol{x})) \mid \boldsymbol{x} \in F_2^n\},$$

$$G_{S'} = \{(\boldsymbol{x}, S'(\boldsymbol{x})) \mid \boldsymbol{x} \in F_2^n\},$$

且存在一个仿射置换 $L: F_2^{2n} \to F_2^{2n}$, 使得

$$L(G_S) = G_S',$$

则称 S 和 S' 满足 Carlet-Charpin-Zinoviev 等价,简称 CCZ 等价。

线性置换 $L: F_2^{2n} \to F_2^{2n}$ 可以看成是一对线性函数 $L_1, L_2: F_2^{2n} \to F_2^n$,对于任意的 $\boldsymbol{x}, \boldsymbol{y} \in F_2^n$ 满足

$$L(\boldsymbol{x}, \boldsymbol{y}) = (L_1(\boldsymbol{x}, \boldsymbol{y}), L_2(\boldsymbol{x}, \boldsymbol{y}))。$$

那么对于一个函数 $S: F_2^n \to F_2^n$, 得到

$$L(\boldsymbol{x}, S(\boldsymbol{x})) = (L_1(\boldsymbol{x}, S(\boldsymbol{x})), L_2(\boldsymbol{x}, S(\boldsymbol{x}))),$$

其中:

$$S_1(\boldsymbol{x}) = L_1(\boldsymbol{x}, S(\boldsymbol{x})) \tag{1}$$

$$S_2(\boldsymbol{x}) = L_2(\boldsymbol{x}, S(\boldsymbol{x})) \tag{2}$$

因此,集合

$$L(G_S) = \{(S_1(\boldsymbol{x}), S_2(\boldsymbol{x})) : \boldsymbol{x} \in F_2^n\}$$

是函数 S' 的图像当且仅当函数 S_1 是一个置换。如果 L 和 S_1 是置换即有 $L(G_S) = G_{S'}$,其中,$S' = S_2 \circ S_1^{-1}$, 即 S 和 S' CCZ 等价。

从定义 8 和 9 可以看到仿射等价是一种特殊的 EA 等价,然后 EA 等价又是一种特殊的 CCZ 等价。

引理 1[5]　如果 $\sigma \in O_n(F_2)$, 则对于任意的 $\boldsymbol{a}, \boldsymbol{b} \in F_2^n, \sigma(\boldsymbol{x} \oplus \boldsymbol{a}) \oplus \boldsymbol{b}$ 也为 F_2^n 上的正形置换。

从引理 1 可以看到,正形置换的个数必为 2^n 的倍数。

引理 2　如果 $\sigma \in LO_n(F_2)$, 当且仅当存在一个 F_2 上的 n 阶矩阵 $\boldsymbol{A}$,满足 $|\boldsymbol{A}| \neq 0, |\boldsymbol{A} + \boldsymbol{I}_n| \neq 0$(也就是矩阵 $\boldsymbol{A}$ 的特征值不为 0 和 1),使得 $\sigma(\boldsymbol{x}) = \boldsymbol{A}\boldsymbol{x}$,其中,$\boldsymbol{I}_n$ 表示 n 阶单位矩阵。

文中称这种矩阵为 F_2 上的 n 阶正形矩阵。

可以看到,F_2^n 上的线性正形置换与 F_2 上的 n 阶正形矩阵存在着一一对应的关系。

引理 3[11]　如果 $\sigma \in MLO_n(F_2)$, 当且仅当 σ 的特征多项式为 F_2 上的 n 次本原多项式。

引理 4[13]　对于 $F_2^n \to F_2^n$ 上的任意映射 S,那么差分均匀度、有差分均匀度和非线性度是 CCZ 等价不变量,代数次数是仿射等价不变量,并且当映射 S 不为仿射变换时,代数次数相对于 S 和 $A_1 \circ S \circ A_2 + A_3$ 是 EA 等价不变量。

2　一个结论的修正以及最大线性正形置换的无重复构造

文献[9] 中给出了 F_2^n 上线性正形置换的一种完全无重复的构造方法,但是其中一些结论的表述上存在问题。

为了便于阅读,结合文献[9] 中的内容,将其中一些符号表示和结论陈列如下:

首先是一些要用到的符号。

$M_{s,t}(F_2)$:表示 F_2 上的 $s \times t$ 阶矩阵所组成的集合;

$GL_s(F_2)$:F_2 上的 s 阶可逆方阵所组成的集合;

$OM_s(F_2)$:F_2 上的 s 阶正形方阵所组成的集合;

$$\boldsymbol{e}_1 = (1, 0, \cdots, 0)^{\mathrm{T}} \in M_{n,1}(F_2);$$

$$\boldsymbol{J}(a_0, a_1, \cdots, a_{r-1}) = \begin{pmatrix} 0 & & & & a_0 \\ 1 & 0 & & & \\ & 1 & \ddots & & \\ & & \ddots & 0 & a_{r-2} \\ & & & 1 & a_{r-1} \end{pmatrix},$$

其中, $a_i \in F_2, 0 \leq i < r$。

接着是文献[9]中的一个引理:

引理 5

1) $\boldsymbol{J}(a_0, a_1, \cdots, a_{r-1}) = \begin{pmatrix} 0 & & & & a_0 \\ 1 & 0 & & & \\ & 1 & \ddots & & \\ & & \ddots & 0 & a_{r-2} \\ & & & 1 & a_{r-1} \end{pmatrix}$,

则 $\boldsymbol{J}(a_0, a_1, \cdots, a_{r-1}) \in OM_r(F_2)$ 当且仅当 $a_0 = 1$ 并且 $\sum_{i=0}^{r-1} a_i = 1$;

2) $\begin{pmatrix} \boldsymbol{A}_1 & \boldsymbol{B} \\ 0 & \boldsymbol{A}_2 \end{pmatrix}$ 是一个正形矩阵当且仅当 $\boldsymbol{A}_1$ 和 $\boldsymbol{A}_2$ 都为正形矩阵;

3) $\boldsymbol{A} \in OM_r(F_2)$ 当且仅当存在 $\boldsymbol{K} \in GL_r(F_2)$ 使得 $\boldsymbol{K}\boldsymbol{A}\boldsymbol{K}^{-1} \in OM_r(F_2)$。

接下来是文献[9] 中 2 个有问题的结论:

结论 1　假设 $\boldsymbol{A} \in M_{n,n}(F_2), \boldsymbol{\delta}_0, \boldsymbol{\delta}_1, \cdots, \boldsymbol{\delta}_{r-1} \in F_2^n$ 并且线性无关,其中,$\boldsymbol{\delta}_0 = \boldsymbol{e}_1, \boldsymbol{D}_0 = (\boldsymbol{e}_1, \boldsymbol{\delta}_1, \cdots, \boldsymbol{\delta}_{r-1}) \in M_{n,r}(F_2)$。选取一个矩阵 $\boldsymbol{D}_1 \in M_{r,n}(F_2)$ 使得 $\boldsymbol{D}_* = (\boldsymbol{D}_0 \boldsymbol{D}_1) \in GL_n(F_2)$。则有:

1) $\boldsymbol{A}^i \boldsymbol{e}_1 = \boldsymbol{\beta}_i, 1 \leq i < r$,

$$\boldsymbol{A}^r \boldsymbol{e}_1 = \sum_{i=0}^{r-1} a_i \boldsymbol{A}^i \boldsymbol{e}_1, a_i \in F_2 \tag{3}$$

当且仅当 $\boldsymbol{A}$ 的形式为:

$$\boldsymbol{D}_* \begin{pmatrix} \boldsymbol{J}(a_0, \cdots, a_{r-1}) & \boldsymbol{B} \\ 0 & \boldsymbol{G} \end{pmatrix} \boldsymbol{D}_*^{-1} \tag{4}$$

其中, $\boldsymbol{B} \in M_{r,n-r}(F_2), \boldsymbol{G} \in OM_{n-r}(F_2)$。

2)$\boldsymbol{A} \in OM_n(F_2)$ 并且满足式(3)当且仅当 $\boldsymbol{A}$ 的形式满足式(4),同时 $a_0 = 1$,并且 $\sum_{i=1}^{r-1} a_i = 1$,$\boldsymbol{G} \in OM_{n-r}(F_2)$。

结论2 $OM_n(F_2) =$

$$\bigcup_{\substack{2\le r\le n\\ r\ne n-1}} \bigcup_{\boldsymbol{D}_*\in D_r} \bigcup_{\substack{(a_1,\cdots,a_{r-1})\in F_2^{r-1}\\ \sum_{i=1}^{r-1}a_i=1\\ \boldsymbol{B}\in M_{r,n-r}(F_2)}} \boldsymbol{D}_* OM_{n,r}(a_1,\cdots,a_{r-1},\boldsymbol{B})\boldsymbol{D}_*^{-1}。$$

其中,

$$D_r = \left\{ \boldsymbol{D}_* = (\boldsymbol{D}\boldsymbol{D}_1) \left| \begin{array}{l} \boldsymbol{D} = (\boldsymbol{e}_1\Delta) \in M_{n,r}(F_2),\\ \mathrm{rank}(\boldsymbol{D}) = r。\\ 对每个\ D\ 选取一个\\ \boldsymbol{D}_1 \in M_{r,n}(F_2),使得\\ \boldsymbol{D}_* = (\boldsymbol{D}\boldsymbol{D}_1) \in GL_n(F_2) \end{array} \right. \right\}。$$

其中,

$$OM_{n,r}(a_1,\cdots,a_{r-1},\boldsymbol{B}) = \left\{ \begin{pmatrix} \boldsymbol{J}(1,a_1,\cdots,a_{r-1}) & \boldsymbol{B}\\ 0 & \boldsymbol{G} \end{pmatrix} \boldsymbol{G} \in OM_{n-r}(F_2) \right\},$$

并且

$$\boldsymbol{D}_* OM_{n,r}(a_1,\cdots,a_{r-1},\boldsymbol{B})\boldsymbol{D}_*^{-1} = \{\boldsymbol{D}_*\boldsymbol{A}\boldsymbol{D}_*^{-1} \mid \boldsymbol{A} \in OM_{n,r}(a_1,\cdots,a_{r-1},\boldsymbol{B})\}。$$

作者认为:

结论1中的"选取一个矩阵 $\boldsymbol{D}_1 \in M_{r,n}(F_2)$ 使得 $\boldsymbol{D}_* = (\boldsymbol{D}_0\boldsymbol{D}_1) \in GL_n(F_2)$"存在问题。按照结论1中"$\boldsymbol{\delta}_0,\boldsymbol{\delta}_1,\cdots,\boldsymbol{\delta}_{r-1} \in F_2^n$ 并且线性无关"的描述,可以得到 $r \le n$,并且 $\mathrm{rank}(\boldsymbol{D}_0) = r$;因为 $\boldsymbol{D}_1 \in M_{r,n}(F_2)$,$r \le n$,所以得到 $\mathrm{rank}(\boldsymbol{D}_1) \le r$。而大家知道:$\mathrm{rank}(\boldsymbol{D}_*) = \mathrm{rank}(\boldsymbol{D}_0\boldsymbol{D}_1) \le \min\{\mathrm{rank}(\boldsymbol{D}_0), \mathrm{rank}(\boldsymbol{D}_1)\}$,所以得到 $\mathrm{rank}(\boldsymbol{D}_*) \le \mathrm{rank}(\boldsymbol{D}_1) \le r$。又因为"$\boldsymbol{D}_* \in GL_n(F_2)$",所以 $\mathrm{rank}(\boldsymbol{D}_*) = n$。这样又得到了 $n \le r$。综合 $r \le n$ 与 $n \le r$,得到 r 必须和 n 相等。这样结论1就变成了如下的结论3:

结论3 假设 $\boldsymbol{A} \in M_{n,n}(F_2)$,$\boldsymbol{\delta}_0,\boldsymbol{\delta}_1,\cdots,\boldsymbol{\delta}_{n-1} \in F_2^n$ 并且线性无关,其中,$\boldsymbol{\delta}_0 = \boldsymbol{e}_1$,$\boldsymbol{D}_0 = (\boldsymbol{e}_1,\boldsymbol{\delta}_1,\cdots,\boldsymbol{\delta}_{n-1}) \in M_{n,n}(F_2)$。选取一个矩阵 $\boldsymbol{D}_1 \in M_{n,n}(F_2)$ 使得 $\boldsymbol{D}_* = (\boldsymbol{D}_0\boldsymbol{D}_1) \in GL_n(F_2)$。则有:

1)$\boldsymbol{A}^i\boldsymbol{e}_1 = \boldsymbol{\beta}_i$,$1 \le i < n$,

$$\boldsymbol{A}^n\boldsymbol{e}_1 = \sum_{i=0}^{n-1} a_i\boldsymbol{A}^i\boldsymbol{e}_1, a_i \in F_2 \tag{5}$$

当且仅当 $\boldsymbol{D}$ 的形式为:

$$\boldsymbol{D}_*\boldsymbol{J}(a_0,\cdots,a_{n-1})\boldsymbol{D}_*^{-1} \tag{6}$$

2)$\boldsymbol{A} \in OM_n(F_2)$ 并且满足式(5)当且仅当 $\boldsymbol{A}$ 的形式满足式(6),同时 $a_0 = 1$,并且 $\sum_{i=1}^{n-1} a_i = 1$。

同样可以对结论2分析得到等价的结论4:

结论4 $OM_n(F_2) =$

$$\bigcup_{\boldsymbol{D}_*\in D_n} \bigcup_{\substack{(a_1,\cdots,a_{n-1})\in F_2^{n-1}\\ \sum_{i=1}^{n-1}a_i=1}} \boldsymbol{D}_* OM_{n,n}(a_1,\cdots,a_{n-1})\boldsymbol{D}_*^{-1}。$$

其中,

$$D_n = \left\{ \boldsymbol{D}_* = (\boldsymbol{D}\boldsymbol{D}_1) \left| \begin{array}{l} \boldsymbol{D} = (\boldsymbol{e}_1\Delta) \in GL_n(F_2),\\ 对每个\ \boldsymbol{D}\ 选取一个\\ \boldsymbol{D}_1 \in M_{n,n}(F_2),使得\\ \boldsymbol{D}_* = (\boldsymbol{D}\boldsymbol{D}_1) \in GL_n(F_2) \end{array} \right. \right\}。$$

其中,

$$OM_{n,n}(a_1,\cdots,a_{n-1}) = \{\boldsymbol{J}(1,a_1,\cdots,a_{n-1})\},$$

并且

$$\boldsymbol{D}_* OM_{n,n}(a_1,\cdots,a_{n-1})\boldsymbol{D}_*^{-1} = \{\boldsymbol{D}_*\boldsymbol{A}\boldsymbol{D}_*^{-1} \mid \boldsymbol{A} \in OM_{n,n}(a_1,\cdots,a_{n-1})\}。$$

那么按照结论4,得到

$|D_n| = \prod_{i=2}^{n}(2^n - 2^{-1})$ 和 $|OM_{n,n}(a_1,\cdots,a_{n-1})| = 2^{n-2}$,进而得到 $|OM_n(F_2)| = \prod_{i=2}^{n}(2^n - 2^{-1}) \cdot 2^{n-2}$,这与已知的结果[14]是相违背的,因此可以看到结论3以及4存在问题,进而结论1和2存在问题。

结论1按如下修正即可:

引理6 假设 $\boldsymbol{A} \in M_{n,n}(F_2)$,$\boldsymbol{\delta}_0,\boldsymbol{\delta}_1,\cdots,\boldsymbol{\delta}_{r-1} \in F_2^n$ 并且线性无关,其中,$\boldsymbol{\delta}_0 = \boldsymbol{e}_1$,$\boldsymbol{D}_0 = (\boldsymbol{e}_1,\boldsymbol{\delta}_1,\cdots,\boldsymbol{\delta}_{r-1}) \in M_{n,r}(F_2)$ $(r < n)$。选取一组 $\boldsymbol{\delta}_r,\boldsymbol{\delta}_{r+1},\cdots,\boldsymbol{\delta}_{n-1} \in F_2^n$ 使得 $\boldsymbol{D}_* = (\boldsymbol{\delta}_0,\cdots,\boldsymbol{\delta}_{r-1},\boldsymbol{\delta}_r,\boldsymbol{\delta}_{r+1},\cdots,\boldsymbol{\delta}_{n-1}) \in GL_n(F_2)$。当 $r = n$ 时,取 $\boldsymbol{D}_* = \boldsymbol{\delta}_0$。则有:

1)$\boldsymbol{A}\boldsymbol{\delta}_{i-1} = \boldsymbol{\delta}_i$,$1 \le i < r$,

$$\boldsymbol{A}\boldsymbol{\delta}_{r-1} = \sum_{i=0}^{r-1} a_i\boldsymbol{\delta}_i, a_i \in F_2 \tag{7}$$

当且仅当 $\boldsymbol{A}$ 的形式为:

$$\boldsymbol{D}_* \begin{pmatrix} \boldsymbol{J}(a_0,\cdots,a_{r-1}) & \boldsymbol{B}\\ 0 & \boldsymbol{G} \end{pmatrix} \boldsymbol{D}_*^{-1} \tag{8}$$

其中,$\boldsymbol{B} \in M_{r,n-r}(F_2)$,$\boldsymbol{G} \in M_{n-r,n-r}(F_2)$。

2)$\boldsymbol{A} \in OM_n(F_2)$ 并且满足式(7)当且仅当 $\boldsymbol{A}$ 的形式满足式(8),同时 $a_0 = 1$,并且 $\sum_{i=1}^{r-1} a_i = 1$,$\boldsymbol{G} \in OM_{n-r}(F_2)$。

证明:当已知一个满足引理6中描述的 $\boldsymbol{D}_0$ 时,根据线性代数的知识,得到

$$|\{(\boldsymbol{\delta}_r,\cdots,\boldsymbol{\delta}_{n-1}) \mid \boldsymbol{D}_* = (\boldsymbol{e}_1,\cdots,\boldsymbol{\delta}_{r-1},\boldsymbol{\delta}_r,\cdots,\boldsymbol{\delta}_{n-1}) \in GL_n(F_2)\}| = \prod_{i=r+1}^{n}(2^n - 2^{i-1}) \quad (r < n)。$$

因此当 $r < n$ 时,引理6 中也存在 $\boldsymbol{\delta}_r, \boldsymbol{\delta}_{r+1}, \cdots, \boldsymbol{\delta}_{n-1} \in F_2^n$ 满足 $\boldsymbol{D}_*$ 的构造。

1) 必要性。如果式(7) 成立,则有

$\boldsymbol{AD}_0 = \boldsymbol{D}_0 \boldsymbol{J}(a_0, a_1, \cdots, a_{r-1})$,进而得到

$$\boldsymbol{AD}_* = \boldsymbol{D}_* \begin{pmatrix} \boldsymbol{J}(a_0, a_1, \cdots, a_{r-1}) & \boldsymbol{B} \\ 0 & \boldsymbol{G} \end{pmatrix}。$$

其中,$\boldsymbol{B} \in M_{r,n-r}(F_2)$, $\boldsymbol{G} \in M_{n-r,n-r}(F_2)$。

充分性同理可证。

2) 充分性。由引理5 中的结论1、2、3,充分性可得。

必要性同理可证。

结论2 按如下修正:

定理 1　$OM_n(F_2) =$

$$\bigcup_{\substack{2 \le r \le n \\ r \ne n-1}} \bigcup_{\boldsymbol{D}_* \in D_r} \bigcup_{\substack{(a_1, \cdots, a_{r-1}) \in F_2^{r-1} \\ \sum_{i=1}^{r-1} a_i = 1 \\ \boldsymbol{B} \in M_{r,n-r}(F_2)}} \boldsymbol{D}_* OM_{n,r}(a_1, \cdots, a_{r-1}, \boldsymbol{B}) \boldsymbol{D}_*^{-1}。$$

其中,

$$D_r = \left\{ \boldsymbol{D}_* = (\boldsymbol{e}_1 \boldsymbol{\Delta}) \;\middle|\; \begin{array}{l} \boldsymbol{D} = (\boldsymbol{e}_1, \cdots, \boldsymbol{\delta}_{r-1}) \in \\ M_{n,r}(F_2), \\ \mathrm{rank}(\boldsymbol{D}) = r。对每个 \boldsymbol{D} 取 \\ \boldsymbol{\delta}_r, \boldsymbol{\delta}_{r+1}, \cdots, \boldsymbol{\delta}_{n-1} \in F_2^n, 使 \\ \boldsymbol{D}_* = (\boldsymbol{e}_1, \cdots, \boldsymbol{\delta}_{r-1}, \boldsymbol{\delta}_r, \cdots, \\ \boldsymbol{\delta}_{n-1}) \in GL_n(F_2)。当 r = n \\ 时,取 \boldsymbol{D}_* = \boldsymbol{D}。 \end{array} \right\}。$$

其中,

$$OM_{n,r}(a_1, \cdots, a_{r-1}, \boldsymbol{B}) = \left\{ \begin{pmatrix} \boldsymbol{J}(1, a_1, \cdots, a_{r-1}) & \boldsymbol{B} \\ 0 & \boldsymbol{G} \end{pmatrix} \boldsymbol{G} \in OM_{n-r}(F_2) \right\},$$

并且

$$\boldsymbol{D}_* OM_{n,r}(a_1, \cdots, a_{r-1}, \boldsymbol{B}) \boldsymbol{D}_*^{-1} = \{ \boldsymbol{D}_* \boldsymbol{A} \boldsymbol{D}_*^{-1} \mid \boldsymbol{A} \in OM_{n,r}(a_1, \cdots, a_{r-1}, \boldsymbol{B}) \}。$$

证明:根据引理6,将 r 从2 取到 n,命题可得。

根据定理1,可得

$$\mid OM_n(F_2) \mid = \sum_{r=2}^{n} \mid \{(\boldsymbol{\delta}_1, \cdots, \boldsymbol{\delta}_{r-1})\} \mid \cdot \mid \{(a_0, \cdots, a_{r-1})\} \mid \cdot \mid \{\boldsymbol{B}\} \mid \cdot \mid \{\boldsymbol{G}\} \mid = \sum_{r=2}^{n} \prod_{i=2}^{r} (2^n - 2^{i-1}) \cdot 2^{r-2} \cdot 2^{r(n-r)} \cdot \mid OM_{n-r}(F_2) \mid,$$

这和文献[14] 中的结果一致。

最大线性正形置换是一类特殊的线性正形置换,可以利用最大线性正形置换构造密码性能较好的非线性正形置换。

文献[11] 中给出了最大线性正形置换的计数公式,也给出了构造方法,但是该方法并不是一个完全无重复的构造方法,会产生很多重复的结果(每一个结果会重复 $2^n - 1$ 次),下面结合定理1,给出一种完全无重复的 F_2^n 上最大线性正形置换的构造方法。

定理 2　F_2^n 上的最大线性正形置换,所对应的矩阵形式均为

$$(\boldsymbol{\delta}_0, \cdots, \boldsymbol{\delta}_{n-1}) \begin{pmatrix} 0 & & & & 1 \\ 1 & 0 & & & \\ & \ddots & & & \\ & & & 0 & a_{n-2} \\ & & & 1 & a_{n-1} \end{pmatrix} (\boldsymbol{\delta}_0, \cdots, \boldsymbol{\delta}_{n-1})^{-1}。$$

其中,$\boldsymbol{\delta}_0 = \boldsymbol{e}_1, \boldsymbol{\delta}_1, \cdots, \boldsymbol{\delta}_{n-1} \in F_2^n$,并且 $(\boldsymbol{\delta}_0, \cdots, \boldsymbol{\delta}_{n-1}) \in GL_n(F_2)$,特征多项式为:

$f(x) = x^n + \sum_{i=1}^{n-1} a_{n-1} x^i + 1$,且 $f(x)$ 为 F_2 上的 n 次本原多项式。

证明:由定理1 可知

$$OM_n(F_2) = \bigcup_{\substack{2 \le r \le n \\ r \ne n-1}} \bigcup_{\boldsymbol{D}_* \in D_r} \bigcup_{\substack{(a_1, \cdots, a_{r-1}) \in F_2^{r-1} \\ \sum_{i=1}^{r-1} a_i = 1 \\ \boldsymbol{B} \in M_{r,n-r}(F_2)}} \boldsymbol{D}_* OM_{n,r}(a_1, \cdots, a_{r-1}, \boldsymbol{B}) \boldsymbol{D}_*^{-1}。$$

而对于一组给定的 $r, \boldsymbol{D}_*, (a_1, \cdots, a_{r-1}), \boldsymbol{B}, \boldsymbol{G}$ 来说,正形矩阵 $\boldsymbol{D}_* \begin{pmatrix} \boldsymbol{J}(1, a_1, \cdots, a_{r-1}) & \boldsymbol{B} \\ 0 & \boldsymbol{G} \end{pmatrix} \boldsymbol{D}_*^{-1}$ 与 $\begin{pmatrix} \boldsymbol{J}(1, a_1, \cdots, a_{r-1}) & \boldsymbol{B} \\ 0 & \boldsymbol{G} \end{pmatrix}$ 互为相似矩阵,所以二者的特征多项式相同。由引理3 可以看到,最大正形置换多项式的特征多项式为本原多项式,本原多项式是一种特殊的不可约多项式,对应到矩阵 $\begin{pmatrix} \boldsymbol{J}(1, a_1, \cdots, a_{r-1}) & \boldsymbol{B} \\ 0 & \boldsymbol{G} \end{pmatrix}$ 中,所以必要条件之一是 r 必须为 n。这样最大正形置换对应的矩阵形式必须为:

$$(\boldsymbol{\delta}_0, \cdots, \boldsymbol{\delta}_{n-1}) \begin{pmatrix} 0 & & & & 1 \\ 1 & 0 & & & \\ & \ddots & & & \\ & & & 0 & a_{n-2} \\ & & & 1 & a_{n-1} \end{pmatrix} (\boldsymbol{\delta}_0, \cdots, \boldsymbol{\delta}_{n-1})^{-1},$$

特征多项式为 $x^n + \sum_{i=1}^{n-1} a_{n-1} x^i + 1$,且该多项式为 F_2 上的 n 次本原多项式。命题得证。

所以只需要枚举 F_2 上的 n 次本原多项式,同时枚举 δ_1 到 δ_{n-1} 就可以完全无重复的构造 F_2^n 上的最大线性正形置换。同时可以得到 F_2^n 上的最大线性正形置换的计数为:

$$|MLO_n(F_2)| = \frac{\varphi(2^n-1)}{n}\prod_{i=2}^{n}(2^n-2^{i-1}) =$$

$$\frac{\varphi(2^n-1)}{n}\cdot\prod_{i=1}^{n-1}2^i(2^{n-i}-1) =$$

$$\frac{\varphi(2^n-1)}{n}\cdot 2^{\frac{n(n-1)}{2}}\cdot\prod_{i=1}^{n-1}(2^{n-i}-1) =$$

$$\frac{\varphi(2^n-1)}{n}\cdot 2^{\frac{n(n-1)}{2}}\cdot\prod_{i=1}^{n-1}(2^i-1),$$

和文献[11]中的计数结果一致。

3 一个关于计数的新结论

讨论正形置换和它的补置换之间的关系。

定理3 若 $\sigma\in O_n(F_2)$,则 σ 的补置换 $S(\boldsymbol{x})=(\boldsymbol{x})\oplus\boldsymbol{x}$ 和任意的 $\sigma(\boldsymbol{x}\oplus\boldsymbol{a})\oplus\boldsymbol{b}(\boldsymbol{a},\boldsymbol{b}\in F_2^n)$ 都不相同。

证明:反证法。假设存在 $\sigma\in O_n(F_2)$,满足 $\sigma(\boldsymbol{x})\oplus\boldsymbol{x}=\sigma(\boldsymbol{x}\oplus\boldsymbol{a})\oplus\boldsymbol{b}$,则对于 $\boldsymbol{x}_1\in F_2^n$,有 $\sigma(\boldsymbol{x}_1)\oplus\boldsymbol{x}_1=\sigma(\boldsymbol{x}_1\oplus\boldsymbol{a})\oplus\boldsymbol{b}$。现在设

$$\boldsymbol{x}_2=\boldsymbol{x}_1\oplus\boldsymbol{a},$$

则有

$$\sigma(\boldsymbol{x}_2\oplus\boldsymbol{a})\oplus\boldsymbol{x}_2\oplus\boldsymbol{a}=\sigma(\boldsymbol{x}_2)\oplus\boldsymbol{b},$$

即

$$\sigma(\boldsymbol{x}_2)\oplus\boldsymbol{x}_2=\sigma(\boldsymbol{x}_2\oplus\boldsymbol{a})\oplus\boldsymbol{b}\oplus\boldsymbol{a}。$$

所以 $\boldsymbol{a}$ 必须为0。但若 $\boldsymbol{a}=0$,代入

$$\sigma(\boldsymbol{x})\oplus\boldsymbol{x}=\sigma(\boldsymbol{x}\oplus\boldsymbol{a})\oplus\boldsymbol{b},$$

得到 $\boldsymbol{x}$ 必须等于 $\boldsymbol{b}$,与假设的 $\sigma\in O_n(F_2)$ 相矛盾,所以命题得证。

定理4 F_2^n 上正形置换的个数必为 2^{n+1} 的倍数。

证明:如果 $\sigma\in O_n(F_2)$,由定理3可知 $\sigma(\boldsymbol{x})\oplus\boldsymbol{x}$ 和任意的 $\sigma\oplus\boldsymbol{a}(\boldsymbol{a}\in F_2^n)$ 都不相同,进而 $\sigma(\boldsymbol{x})\oplus\boldsymbol{x}\oplus\boldsymbol{b}(\boldsymbol{b}\in F_2^n)$ 和任意的 $\sigma\oplus\boldsymbol{a}(\boldsymbol{a}\in F_2^n)$ 都不相同,即存在一个 $\sigma\in O_n(F_2)$,就可以得到 2^{n+1} 个互不相同的正形置换,所以命题得证。

4 正形置换和它的补置换的密码学性质

多输出函数的常见密码学性质除了第1节中给出的非线性度、差分均匀度以及代数次数之外,还需要衡量该多输出函数对抗代数攻击的能力,给出如下的代数免疫度的定义:

定义10 设 $n\times m$ 多输出函数

$$A(\boldsymbol{x})=(A_0(\boldsymbol{x}),\cdots,A_{m-1}(\boldsymbol{x})),$$

其中,$\boldsymbol{x}=(x_0,\cdots,x_{n-1})\in F_2^n$,$P$ 是包含所有形如

$$P(x_0,\cdots x_{n-1},A_0,\cdots,A_{m-1}) =$$

$$\sum a_{ij}x_iA_j\oplus\sum b_{ij}x_ix_j\oplus\sum c_{ij}A_iA_j\oplus$$

$$\sum d_ix_i\oplus\sum e_jA_j\oplus g=0 \qquad (9)$$

的多变量等式的集合(次数不超过2),t 是方程组中出现的所有的单项式的个数(加上常数项),r 代表 P 中两两线性无关的等式的数量,那么

$$AI(A)=(t-r)$$

为 A 的代数免疫度。

备注:由于目前对于多输出函数的代数免疫度还缺乏统一的定义,所以定义 $(t-r)$ 为一个 $n\times m$ 多输出函数的代数免疫度。这个定义也是源自文献[15]中定义的对于一个 $n\times n$ 的置换盒的攻击复杂度 $((t-r)/n)^{\lceil(t-r)/n\rceil}$。

根据定义10可以看到,一个 $n\times m$ 多输出函数 A 的代数免疫度有如下上界:

$$AI(A)\le\min\{2^n,\binom{n}{2}+\binom{m}{2}+nm+n+m+1\}。$$

定理5 定义的代数免疫度是CCZ等价不变量。

证明:假设 $F_2^n\to F_2^n$ 上的映射 S 和 S' 是CCZ等价,那么就有 $S'=S_2\circ S_1^{-1}$,其中,S_1 和 S_2 是针对一个仿射置换 $L=(L_1,L_2)$,按照式(1)和(2)中来定义的。现在若对于 S,存在一个形如式(9)的等式 p 可以用于代数攻击:

$$p(\boldsymbol{x},S(\boldsymbol{x}))=0,$$

那么 $p\circ L^{-1}$ 和 p 的次数相同,并有

$$p\circ L^{-1}(S_1(\boldsymbol{x}),S_2(\boldsymbol{x}))=0,$$

设 $\boldsymbol{x}'=S_1(\boldsymbol{x})$,则得到

$$p\circ L^{-1}(\boldsymbol{x}',S'(\boldsymbol{x}'))=0。$$

该等式可以用来对 S' 进行代数攻击,所以对应 S 的代数攻击的等式都可以转化为对应 S' 的代数攻击的等式,反之亦然。所以二者等式中的两两线性无关的等式数量相等,进而两者的代数免疫度相等,命题得证。

定理6 如果 $\sigma\in O_n(F_2)$ 且 σ 不为仿射正形置换,则 σ 与它的补置换 $\sigma(\boldsymbol{x})\oplus\boldsymbol{x}$ 的差分均匀度,非线性度,代数次数和代数免疫度均相等。

证明:σ 与它的补置换 $\sigma(\boldsymbol{x})\oplus\boldsymbol{x}$ 是 EA 等价,由引理4和定理5,结论可得。

5 结 论

主要是通过对正形置换的构造计数以及密码学性质进行分析,得出了一些新的结论:

引理 6 和定理 1 修正了原先结论关于线性正形置换结构描述方面存在的问题。定理 2 则基于修正后线性正形置换的结构特点,给出了最大线性正形置换的结构,这样基于定理 2 就可以实现最大线性正形置换的完全无重复构造。定理 3 和 4 则通过分析正形置换的补置换和仿射正形置换的关系,得到正形置换的个数为 2^{n+1} 的倍数的新结论。定理 5 证明了文中定义的代数免疫度是 CCZ 等价不变量,定理 6 基于定理 5 得出了非仿射正形置换与它的补置换,包括代数免疫度在内四项密码学指标均相等的结论。

正形置换的密码学性质分析还需要在未来得到进一步的关注。

参考文献:

[1] Mittenthal L. Block substitutions using orthomorphic mappings[J]. Advances in Applied Mathematics,1995,16(1):59 – 71.

[2] Feng Dengguo, Feng Xiutao, Zhang Wentao, et al. Loiss: A byte-oriented stream cipher[C]//Processings of the 3rd International Workshop on Coding and Cryptology. Berlin: Springer,2011:109 – 125.

[3] Tong Yan, Zhang Huanguo. Hybrid strategy of particle swarm optimization and simulated annealing for optimizing orthomorphisms[J]. China Communications, 2012, 9(1):49 – 57.

[4] Diffie W, Ledin G. SMS4 encryption algorithm for wireless networks[EB/OL]. (2008 – 7 – 29)[2013 – 4 – 30]. http://eprint. iacr. org/2008/329.

[5] 吕述望,范修斌,王昭顺,等. 完全映射及其密码学应用[M]. 安徽:中国科学技术大学出版社,2008.

[6] Ren Jinping, Lv Shuwang. Enumerations and Couting of orthomorphic permutations[J]. Journal of Computer Research and Development,2006,43(6):1071 – 1075. [任金萍,吕述望. 正形置换的枚举与计数[J]. 计算机研究与发展,2006,43(6):1071 – 1075.]

[7] Zheng Haoran, Zhang Haimo, Fan Dong. Correction of construction method of orthomorphic permutations and improvement of its enumeration lower bound[J]. Journal on Communications,2009,30(12):45 – 50. [郑浩然,张海模,樊东. 对一个正形置换构造方法的修正及其计数结果的改进[J]. 通信学报,2009,30(12):45 – 50.]

[8] Zheng Haoran, Zhang Haimo, Cui Ting, et al. A new method for construction of orthomorphic permutations[J]. Journal of Electronics & Information Technology, 2009 (6): 1438 – 1441. [郑浩然,张海模,崔霆,等. 一种新的正形置换构造方法[J]. 电子与信息学报,2009(6):1438 – 1441.]

[9] Dai Zongduo, Golomb S W, Gong Guang. Generating all linear orthomorphisms without repetition[J]. Discrete Mathematics,1999,205(1/2/3):47 – 55.

[10] Tong Yan, Zhang Huanguo, Deng Xiaotie. A kind of more secure orthomorphism generator[J]. Journal of Computer Research and Development,2012,49(8):1655 – 1661. [童言,张焕国,邓小铁. 一种安全性更高的正形置换发生器[J]. 计算机研究与发展,2012,49(8):1655 – 1661.]

[11] Li Zhihui, Li Ruihu, Chen Xiaofeng. Characterization and counting for maximal linear orthomorphisms permutations[J]. Journal of Engineering Mathematics,2002(4):101 – 105. [李志慧,李瑞虎,陈晓峰. 最大线性正形置换的刻画与计数[J]. 工程数学学报,2002(4):101 – 105.]

[12] 吴文玲,冯登国,张文涛. 分组密码的设计与分析[M]. 2 版. 北京:清华大学出版社,2009.

[13] Budaghyan L, Carlet C, Pott A. New classes of almost bent and almost perfect nonlinear polynomials[J]. IEEE Transactions on Information Theory,2006,52(3):1141 – 1152.

[14] Liao Yong, Lu Qijun. Structure and counting of affine orthomophisms[J]. Cryptology and Information, 1996(2):23 – 25. [廖勇,卢起俊. 仿射正形置换结构与计数[J]. 密码与信息,1996(2):23 – 25.]

[15] Courtois N, Pieprzyk J. Cryptanalysis of block ciphers with overdefined systems of equations[C]//Proceedings of the Advances in Cryptology—ASIACRYPT 2002. Berlin: Springer,2002:267 – 287.

(编辑　杨　蓓)