Research Journal of Applied Sciences, Engineering and Technology 5(11): 3074-3078, 2013
DOI:10.19026/rjaset.5.4536
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: August 11, 2012 Accepted: September 17, 2012 Published: April 05, 2013

Research Article

Generalized Linear Orthomorphisms

[1]Haiqing Han, [1]Yanping He and [2]Siru Zhu
[1]Department of Mathematics and Physics, Hubei Polytechnic University, Huangshi 435003, Hubei, China
[2]Department of the Basics, AFRA, Wuhan 430019, Hubei, China

Abstract: In this study, we generalize the conception of orthomorphisms and obtain a counting formula on the generalized linear orthomorphisms over the Galois field with the arbitrary prime number p as the characteristic. Thus the partial generation algorithm of generalized linear orthomorphisms is achieved. The counting formula of the linear orthomorphisms over the finite field with characteristic 2 is the special case in our results. Furthermore, the generalized linear orthomorphisms generated and discussed in this study can gain the maximum branch number when they are designed as P-permutations.

Keywords: Block cipher, generalized linear orthomorphism, p-permutation, the branch number

INTRODUCTION

In modern cryptology, the Feistel and SP structures are two kinds of symmetrical cipher structure with widespread application (Haiqing and Huanguo, 2010). These two structures include both S layer and P layer, where S means the confusion level that consists of several juxtaposed S-boxes and plays an important role of confusion for security safeguard of cryptosystem. Where P layer, the P-permutation refers to the diffusion layer, mainly plays a diffusion role to constitute generally by the linear substitution in the majority situations. For the validity and the usability in the design of cryptosystems, the cryptosystem can be divided into S-box and P-permutation because the design of the modern cryptosystem is getting more and more complex (Huanguo *et al*., 2003). This study defines the over all linear transformation in cryptosystem as the P-permutation.

The orthomorphism is a kind of complete mapping, which has a good crypto logic performance: perfectly balanced (Lohrop, 1995), which becomes one focus of research in the cryptography domain. Teledyne Corporation has developed DSD cryptographic products based on the orthomorphism (Lohrop, 1995). Yusen *et al*. (1999) and Dawu *et al*. (1999) have studied the application of the orthomorphism in the cryptography. The orthomorphisms over the finite field are in widespread application and the current study has focused on the calculation and general algorithm of the orthomorphism. In Yong and Qijun (1996) obtained the counting formula of all linear orthomorphisms over the Galois field F_2^n using the recurrence relation. Zongduo and Solonmen (1999) designed the generation algorithm without repetition of all linear orthomorphisms over the Galois field F_2^n.

At present, taking into account of the specific application of linear orthomorphisms in cryptography the linear orthomorphisms over the finite fields $F_2^8$are very suitable for designing the P-permutation. The important cryptographic indicator to measure the P-permutation is the branch number, the greater the branch number, the better the cryptographic property (Haiqing and Huanguo, 2010). The linear orthomorphisms over the Galois field F_2^8 may be represented by an 8 square matrices (Yun and Hongwei, 2002; Zhihui, 2002). But the square matrices on F_2 treated as the P-permutation can't attain the optimal cryptology nature, because the maximum branch number of matrices below on 8 order will not surpass 5 (Ju-Sung *et al*., 1999).

For certain reason, it is shown that the branch number of the P-permutation ground on linear orthomorphism can't achieve the optimal result. It was found out that the generalized linear orthomorphism may overcome the defect and the calculation formula and constructed algorithm were not recommended. So we have promoted the conception of orthomorphisms in this study and have found the calculation formula on the generalized linear orthomorphism over the general Galois field F_q^n. We have the partial general algorithm of generalized linear orthomorphism.

PRELIMINARIES

Let $F_2 = \{0,1\}$ be a binary finite field. F_{2n} or GF(2^n) is the n-degree extension field of F_2, it also can

Corresponding Author: Yanping He, Department of Mathematics and Physics, Hubei Polytechnic University, Huangshi 435003, Hubei, China

be considered that the n -dimension linear space on F_2. Generally, let F_q be the finite field with an arbitrary prime number characteristic p, namely $q = p^k$. Similarly, F_q^n is the extension field of F_q with degree n.

Definition 1: Let S be a permutation on F_2^n, and I is the identity permutation on F_2^n $(I(x) = x, \forall x \in F_2^n)$. If $S \oplus I$ is still the permutation on F_2^n ($\oplus$ is the addition operation on F_2^n), S is called the orthomorphism on F_2^n. Further, if $\forall X, Y \in F_2^n$ fulfill $S(x+y) = S(x)+S(y)$, S is said to be the linear orthomorphism on F_2^n.

From definition 1, when we consider the orthomorphism on the finite field F_2^n., only F_2^n. is regarded as an additive group. By Reference (Hall and Paige, 1957), if $n \geq 2$, then the orthomorphism on F_2^n. must exist. Definition 1 also shows that a permutation is an orthomorphism if and only if the sum of it and the identity permutation is still a permutation. The finite field F_q^n. is a group for the addition operation, similar to definition 1, the orthomorphisms and linear orthomorphisms can also be definite.

Definition 2: Let A be the reversible matrix on the finite field F_q^n. $(q = p^m$ is prime power, if for all k =1, 2,…, p-1, the matrix $A+kI$ is invertible on F_q. A is said to be the generalized orthomorphic matrix.

Definition 3: Let S be the transformation on the finite field F_q^n. $(q = p^m$ is a prime power) , if for each integer k ($1 \leq k \leq p-1$), $S + kI$ (I is the identity) is still the permutation on the finite field F_q^n. S is called the generalized orthomorphism on the finite field F_q^n.. Further, $\forall x, y \in F_q^n$ hold $S(x+y) = S(x)+S(y)$, S is said to be the generalized linear orthomorphism on F_q^n.

Similar to the Galois field of the characteristic 2, the generalized linear orthomorphism on the Galois field F_q^n and the n square generalized orthomorphic matrix on the finite field F_q are one to one correspondence.

The intention for studying the generalized linear orthomorphisms is to understand their crypto logic properties. In cryptography, when the Generalized Linear orthomorphisms are designed for P-permutation, we take into account about that the main cryptography indicator is the branch number, defined as follows.

Definition 4: Let $P: F_q^n \rightarrow F_q^n$ be a linear transformation, for all $\alpha = (a_1, a_2, \ldots, a_n) \in F_q^n$, let $W_h(\alpha)$ be the number of the non-zero component $a_i (1 \leq i \leq n)$ in α, so $B(P) = \min\limits_{\alpha \neq 0}\{W_h(\alpha) + W_h(P(\alpha))\}$ is called the branch number of the linear transformation P.

Based on the above definition, for any linear transformation $P: F_q^n \rightarrow F_q^n$ there is $B(P) \leq n+1$. According to reference (Ju-Sung *et al.*, 1999), the crypto logic character of the generalized linear orthomorphisms is better than the linear orthomorphisms on F_2^n, so the generalized linear orthomorphisms should be selected to design the P-permutation instead of linear orthomorphism on F_2^n.

MAIN RESULTS

The study of the generalized linear orthomorphisms on F_q^n has focused on counting formula and generation algorithms. Imitating reference (Yong and Qijun, 1996), we have found out the following counting formula.

Proposition 1: Let $LOP_n(q)$ be the set of the all generalized linear orthomorphisms on the finite field F_q^n ($q = p^m$ is a prime power) , if the cardinality of the set $LOP_n(q)$ is denoted $|LOP_n(q)|$, then

$$|LOP_n(q)| = \sum_{k=p}^{n} q^{k(n-k)+k-p}(q-1)^p \prod_{i=1}^{k-1}(q^n - q^i)|LOP_{n-k}(q)|$$

where $n \geq p$, and $|LOP_{n-k}(q)|$ is the number of the all linear orthomorphisms on the finite field $GF(q^{n-k})$. We stipulate $|LOP_0(q)| = 1$, $|LOP_1(q) = 0$, But $|LOP_2(q)|, \ldots, |LOP_{p-1}(q)|$ need to be calculated in addition.

Proof: It just proves the number of generalized orthomorphic matrix can satisfy the above formula. It needs simplifying the notation to help the proof.

Let L_n express the set of the all generalized orthomorphic matrix on the finite field F_q^n.

$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ denote the n dimensional column vectors on F_q and ε_i denotes the vector that the i -st component is1 and the other component is 0. We denote $L_n(\varepsilon_1, \alpha) = \{A \in L_n \mid A\varepsilon_1 = \alpha\}$. If A is the generalized orthomorphic matrix, then $\alpha \neq l\varepsilon_1$ where $l \in F_q$ in accordance with its definition. L_n can be divided into q^n - q classes using α We have the formula:

$$|L_n| = (q^n - q)|L_n(\varepsilon_1, \alpha)|$$

There is one to one correspondence between $L_n(\varepsilon_1, \alpha)$ and $L_n(\varepsilon_1, \varepsilon_2)$ for all $\alpha \in F_q^n$ may be proved. Namely :

$$\varphi: L_n(\varepsilon_1, \alpha) \rightarrow L_n(\varepsilon_1, \varepsilon_2)$$

$$\varphi: A \mapsto B = T^{-1}AT$$

where, $T^{-1}(\varepsilon_1, \alpha, \gamma_3, \dots, \gamma_n)$, $\varepsilon_1, \alpha, \gamma_3, \dots, \gamma_n$ is the basis F_q^nover F_q which is the extension by ε_1, α. It is clear that $T^{-1}\varepsilon_1 = \varepsilon_2 \Longrightarrow T\varepsilon_1 = \varepsilon_1$ And $T^{-1}\varepsilon_2 = \alpha$, that is $T\alpha = \varepsilon_2$, therefore, $B \in L_2(\varepsilon_1, \varepsilon_2)$.
Similarly, when $k \geq 2$, we can define

$$L_n(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k) = \{A \in L_n \mid A\varepsilon_{i-1} = \varepsilon_i, 2 \leq i \leq k\}$$

For $A\varepsilon_k = \alpha$, α can be selected from two sets:

$$\alpha \in F_q^n \setminus span\{\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k\} \tag{1}$$

where $span\{\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k\}$ is the vector space that is span by the linearly independent vectors $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k$;

$$\begin{aligned} &\alpha \in span\{\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k\} \\ &\setminus\{c_2\varepsilon_2 + c_3\varepsilon_3 + \cdots + c_k\varepsilon_k, t\varepsilon_k + d_2(\varepsilon_2 + t\varepsilon_1) \\ &+ \cdots + d_k(\varepsilon_k + t\varepsilon_{k-1}) \mid \\ &c_i, d_i \in F_q, 1 \leq t \leq p-1, 2 \leq i \leq k\} \end{aligned} \tag{2}$$

It is easy to know the number of elements is $(q^n -$ $q^{k)}$ in (1).

The following proofs that the number of elements is $q^{k(n-k)+k-p}(q-1)^p$ in (2).

Since $A\varepsilon_{i-1} = \varepsilon_i, 2 \leq i \leq k$ and $A\varepsilon_k = \alpha = c_1\varepsilon_1 + c_2\varepsilon_2 + c_k\varepsilon_k$, A must have the following form: $\begin{pmatrix} C_k & D \\ O & A_{n-k} \end{pmatrix}$, where, C_k , A_{n-k} denote kand (n-k) square matrix respectively. Calculate C_k and it has the form as follows:

$$\begin{pmatrix} 0 & 0 & \cdots & \cdots & c_1 \\ 1 & 0 & \cdots & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 & c_{k-1} \\ 0 & 0 & \cdots & 1 & c_k \end{pmatrix}$$

The characteristic polynomial of the matrix C_k is

$$f(\lambda) = |\lambda I - C_k| = c_1 + c_2\lambda + \cdots + c_k\lambda^{k-1}.$$

$\begin{pmatrix} C_k & D \\ O & A_{n-k} \end{pmatrix}$ is the generalized orthomorphic matrix if and only if C_k, A_{n-k} is the generalized orthomorphic matrix by the definition of the generalized orthomorphic matrix on F_q, so the characteristic roots of $f(\lambda) = |\lambda I - C_k|$ can't be 0,1,…,(p-1), that is:

$$\begin{cases} f(0) \neq 0 \\ f(1) \neq 0 \\ \quad\vdots \\ f(p-1) \neq 0 \end{cases}$$

where, 0, 1, …, (p − 1) are all in the subfield of F_q as well as in F_q.

Find the number of the solution in following equations system.

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 1 \\ 1 & 2^1 & \cdots & 2^{k-1} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & (p-1) & \cdots & (p-1)^{k-1} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix} = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{p-1} \end{pmatrix}$$

that requirement $a_0, a_1, \dots a_{p-1}$ are all not 0.
$(a_0, a_1, \dots, a_{p-1})^T$ Can be taken $(q-1)^p$ possible values, where $c_1, c_2, \cdots, c_k$ are viewed as unknown variables. The solution of the above equation system exists if and only if that the rank of the augmented matrix equal to the rank of the coefficient matrix. The coefficient matrix is row full rank, so the solution of the above equation systems must exist and the dimension of the solution vectors space is (k-p). There are q^{k-p} solutions $(c_0, c_1, \dots c_k)^T$ given the value $(a_0, a_1, \dots, a_{p-1})^T$, the value $(c_0, c_1, \dots c_k)^T$ has $q^{k-p}(q-1)^p$ classes. Namely, the number of the generalized orthomorphic matrices formed $C_k$is $q^{k-p}(q-1)^p$.

The matrix D in A = $\begin{pmatrix} C_k & D \\ O & A_{n-k} \end{pmatrix}$ has k rows and n – k column, which has $q^{k(n-k)}$ cases to select. It will prove the opinion when α fall in (2). If we denote:

$$\begin{aligned} &L_n(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k, \alpha) = \\ &\{A \in L_n \mid A\varepsilon_{i-1} = \varepsilon_i, A\varepsilon_k = \alpha, 2 \leq i \leq k\} \end{aligned}$$

then the number is:

$$|L_n(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k, \alpha)| = q^{k(n-k)+k-p}(q-1)^p |L_{n-k}|$$

We have obtain the Recurrence relation:

$$|L_n| = (q^n - q)|L_n(\varepsilon_1, \varepsilon_2)|$$

If $k \geq 2$then

$$\begin{aligned} &L_n(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k) = [\bigcup_{\alpha} L_n(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k, \alpha)] \\ &\bigcup_{\beta}[\bigcup L_n(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k, \beta)] \end{aligned}$$

$\cup_\alpha L_n(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k, \alpha)$ denotes that α is taken from (1). Therefore, the counting formula is:

$$\begin{aligned} &|\cup_\alpha L_n(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k, \alpha)| = \\ &\quad (q^n - q^k)|L_n(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{k+1})| \end{aligned}$$

$\bigcup_{\beta} L_n\,(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k, \beta)$ denotes that α is taken from (2).

$$|\bigcup_{\beta} L_n(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k, \beta)| =$$

$$q^{k(n-k)+k-p}(q-1)^p\,|L_{n-k}|$$

Note $L_n(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k, \cdots, \varepsilon_n) = 0$

Summarily,

$$|L_n| = \sum_{k=p}^{n-1} q^{k(n-k)+k-p}(q-1)^p \prod_{i=1}^{k}(q^n - q^i)\,|L_{n-k}|\,(n, k \geq p)$$

we stipulate $|L_0| = 1, |L_1| = 0$ and $|L_2|, \dots, |L_{p-1}|$ need to be calculated separately.

There are two advantages to calculate $|L_2|, \dots, |L_{p-1}|$:

- The order of matrices are relatively small
- The matrix structure with small order can be converted to study the root of the characteristic polynomial that does not exist in the prime subfield F_p of F_q.This proposition is complete.

For example, if p = 3 in the above proposition, | L$_2$ | needs to be calculated, so long as let A = $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in L_2$, Only the number of the polynomials form needs to be calculated.

$$f(\lambda) = |\lambda I - A| = \lambda^2 - (a+b)\lambda + ad - bc$$

Satisfies f(0)$\neq 0, f(1) \neq 1$.

This proposition is the promotion of the conclusion in reference (Yong and Qijun, 1996). If we take q = p = 2then the counting formula of the n square orthomorphic matrices on F_2^n should be obtained.

The generalized orthomorphism on finite fields F_q^ncan be represented and denoted by the permutation polynomials and the multi-output Boolean function. Hence we will give the following conclusions without proof because it is relatively simple.

Proposition 2: Let $f(x)$ be a permutation polynomial on F_q^n, $f(x)$ is the orthomorphic polynomial if and only if $f(x), f(x) + kX(I \leq k \leq p-1)$ are the permutation polynomials.

Proposition 3: Let F(X) be a multi-output Boolean function on F_q^n, F(X) is the orthomorphic multi-output Boolean function if and only if $F(X), F(X) + kI(1 \leq k \leq p-1$ (I is the identity) are the multi-output Boolean functions。

Proposition 4: Let S be a generalized orthomorphism on F_q^n, if Tis an arbitrary linear permutation on F_q^n, then T^{-1}AT is still a generalized orthomorphism.

The conception of the companion matrix can be used to generate a generalized linear orthomorphism.

Let $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \in F_q[x]$

be an irreducible polynomial, the:
$n \times n$ Matrix

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

is said to be the companion matrix of $f(x)$. In the application, the generalized linear orthomorphism on the finite field F_{2^8} is considered and the characteristic is 2. A specific idea is that firstly to find a frobenius canonical matrix, secondly to get a generalized orthomorphic matrix through a similarity transformation, finally to calculate the branch number.

Proposition 5: Let A be the companion matrix of $f(x)$ over the Galois field, if and only if $a_0 \neq 0, a_1 + a_2 + \cdots + a_{n-1} \neq 0$.

From the proposition 1 to the proposition 5, we have got the generation algorithm of the generalized linear orthomorphism of degree n on F_{2^8}, which are as follows:

Algorithm 1:

Step 1: Find an irreducible polynomial $f(x) \in F_{2^8}[x]$ of degree n, or find a manic polynomial $f(x) \in F_{2^8}[x]$ of degree n so that f(0) $\neq 0, f(1) \neq 0$。

Step 2: Write out the companion matrix C$_f$ of the polynomial f(x)

Step 3: Choose any invertible matrix A over F_{2^8} and carry on the similarity transformation C$_f$ to AC_fA^{-1}.

Step 4: Obtain the output AC_fA^{-1}, that is the generalized linear orthomorphism.

Proof and complexity analysis of the algorithm: The companion matrix C$_f$ of the polynomial f(x) must be orthomorphic matrix according to the proof of proposition 1, then AC_fA^{-1} is the generalized linear orthomorphism from proposition 4. The complexity of the algorithm depends on step1 and step3. It needs to determine the irreducibility polynomial f(x) in step1 or demands to judge $f(0)\neq 0, f(1) \neq 0$, which can be completed in polynomial time complexity; The key is to determine the reverse of the matrix A in step3, of which the time complexity is O(n^3). The complexity of the algorithm is not greater than that of the polynomial complexity summing up Step1 and Step3.

Algorithm 2

Step 1: Find two matrices A and C, they are generalized orthomorphic matrices with small order over F_q^n

Step 2 : Find an arbitrary matrix B, make $\begin{pmatrix} C & B \\ O & A \end{pmatrix}$ is a square matrix. Remark the matrix B need not be the square matrix

Step 3 : Choose any invertible matrix P and carry on the similarity transformation $P\begin{pmatrix} C & B \\ O & A \end{pmatrix} P^{-1}$

Proof and complexity analysis of the algorithm will be omit because it is obvious.

CONCLUSION

The study of general linear orthomorphism on the finite field F_2^n has achieved good result , but the generation algorithm of all generalized linear orthomorphisms needs to be studied in depth and the algorithm presented in this study can only generate some linear orthomorphism but not all. Furthermore, the generalized maximum linear orthomorphism (Zhihui, 2004) and the generalized nonlinear orthomorphism need strengthening the study.

In the cryptosystem, the nonlinear parts are important barriers of security threats. The nonlinear component in the design is important that we must fully consider the cryptographic properties and make it resist the linear, differential and algebraic attacks. It's the nonlinear orthomorphisms on GF(2^8) rich raw materials that is the key of designing the non-linear cryptology components. It is the next major task that the generalized linear orthomorphisms on $F_{2^8}^n$ and the nonlinear orthomorphisms on GF(2^8) are used to design the crypto logic algorithms.

ACKNOWLEDGMENT

This study is supported by the national natural science foundation of Hubei Polytechnic University (11YJZ10R) (801-8852).

REFERENCES

Dawu, G., L. Jihong and X. Guozhen, 1999. Construction of cryptographic functions based on orthomorphic permutation. J. XiDian Univ., 26: 40-43(Ch).

Haiqing, H. and Z. Huanguo, 2010. Research on the branch number of P-permutation in block cipher. J. Chinese Comput. Syst., 31: 921-926(Ch).

Hall, M. and L.J. Paige, 1957. Complete mappings of finite groups. Pacific J. Math., 5: 541-549

Huanguo, Z., F. Xiutao, Z. Qin, *et al.*, 2003. Research on evolutionary cryptosystems and evolutionary DES. Chinese J. Comput., 26: 1678-1684(Ch).

Ju-Sung, K., P. Choonsik, L. Sangjin and L. Jong-In, 1999. On the optimal diffusion layers with practical security against differential and linear cryptanalysis. Proceedings of the 2nd International Conference on Information Security and Cryptology, Springer-Verlag, London, pp: 273-283.

Lohrop, M., 1995. Block substitution using orthormorphic mapping. Adv. Appl. Math., 16: 59-71(Ch).

Yong, L. and L. Qijun, 1996. The construction and enumeration of the affine orthemorphisms. J. Ciphers Inform., 2: 23-25, (Ch).

Yusen, X., L. Xiaodong, Y. Yixian, *et al.*, 1999. Constructions and enumerations of orthomorphic permutations in cryptosystem. J. China Inst. Commun., 20: 27-30(Ch).

Yun, F. and L. Hongwei, 2002. Group and Combination Coding. Wuhan University Press, Wuhan, China.

Zhihui, L., 2002. The research on permutation theory in block cipher system. Ph.D. Thesis, Northwestern Polytechnical University, Xi'an, China.

Zhihui, L., 2004. Properties of maximal linear orthemorphisms permutation. J. Shaanxi Normal Univ., Nat. Sci. Edn., 32: 22-24, (Ch).

Zongduo, D. and W.G. Solonmen, 1999. Generating all linear orthemorphisms without repetition. Discrete Math., 5: 47-55.