Generalized Linear Orthomorphisms

Haiqing Han, Yanping He and Siru Zhu

Department of Mathematics and Physics, Hubei Polytechnic University, Huangshi 435003, 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 \(\mathbb{F}_2^n\). 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 be considered that the \(n\)-dimension linear space on \(F_2\).
Generally, let $F_q^n$ be the finite field with an arbitrary prime number characteristic $p$, namely $q = p^n$. Similarly, $F^n_q$ is the extension field of $F_q$ with degree $n$.

**Definition 1:** Let $S$ be a permutation on $F^n_2$, and $I$ is the identity permutation on $F^n_2$ ($I(x) = x, \forall x \in F^n_2$). If $S \oplus I$ is still the permutation on $F^n_2$ ($\oplus$ is the addition operation on $F^n_2$), $S$ is called the orthomorphism on $F^n_2$. Further, if $\forall x, y \in F^n_2$ fulfill $S(x+y) = S(x)+S(y)$, $S$ is said to be the linear orthomorphism on $F^n_2$.

From definition 1, when we consider the orthomorphism on the finite field $F^n_2$, only $F^n_2$ is regarded as an additive group. By Reference (Hall and Paige, 1957), if $n \geq 2$, then the orthomorphism on $F^n_2$ must exist. Definition 1 also shows that a permutation is a permutation if and only if the sum of it and the identity permutation is still a permutation. The finite field $F^n_q$ 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 $F^n_q$, ($q = p^n$ is prime power, if for all $k = 1, 2, \ldots, p-1$, the matrix $A+kl$ is invertible on $F_q$), $A$ is said to be the generalized orhomorphic matrix.

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

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

The intention for studying the generalized orhomorphic 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 $P: F^n_q \rightarrow F^n_q$ be a linear transformation, for all $\alpha = (a_1, a_2, \ldots, a_n) \in F^n_q$, let $W_h(\alpha)$ be the number of the non-zero component $a_i (1 \leq i \leq n)$ in $\alpha$, so $B(P) = \min \{ W_h(\alpha) + W_h(P(\alpha)) \}$ is called the branch number of the linear transformation $P$.

Based on the above definition, for any linear transformation $P: F^n_q \rightarrow F^n_q$ 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 $F^n_2$, so the generalized linear orthomorphisms should be selected to design the P-permutation instead of linear orthomorphism on $F^n_2$.

**MAIN RESULTS**

The study of the generalized linear orthomorphisms on $F^n_q$ 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 all the generalized linear orthomorphisms on the finite field $F^n_q$ ($q = p^n$ is a prime power), if the cardinality of the set $LOP_n(q)$ is denoted $|LOP_n(q)|$, then

$$|LOP_n(q)| = \sum_{i=0}^{n} q^{\binom{n}{k} - i} \cdot (q - 1)^i \cdot \prod_{j=1}^{i} (q^j - q)$$

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

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

Let $L_n$ express the set of all the generalized orhomorphic matrix on the finite field $F^n_q$.

$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ denote the $n$ dimensional column vectors on $F^n_q$ and $\varepsilon_i$ denotes the vector that the $i$-st component is 1 and the other component is 0. We denote $L_n(\varepsilon_i, \alpha) = \{ A \in L_n | A \varepsilon_i = \alpha \}$. If $A$ is the generalized orhomorphic matrix, then $\alpha \neq \lambda \varepsilon_1$ where $\lambda \in F^n_q$ in accordance with its definition. $L_n$ can be divided into $q^n - q$ classes using $\alpha$. 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 $\alpha \in F^n_q$ may be proved. Namely:

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

$$\phi: A \mapsto B = T^{-1}AT$$
where, \( T^{-1}(e_1, \alpha, \gamma_2, \ldots, \gamma_n) \), \( e_1, \alpha, \gamma_2, \ldots, \gamma_n \) is the basis \( F_q^n \) over \( F_q \) which is the extension by \( e_1, \alpha \). It is clear that \( T^{-1}e_1 = \alpha \Rightarrow T\xi_1 = \xi_1 \) and \( T^{-1}e_2 = \alpha \) that is \( T\alpha = e_2 \), therefore, \( B \in L_2(e_1, e_2) \).

Similarly, when \( k \geq 2 \), we can define

\[
L_2(e_1, e_2, \ldots, e_k) = \{ A \in L_n \mid A\xi_i = \xi_i, 2 \leq i \leq k \}
\]

For \( A\xi_k = \alpha \), \( \alpha \) can be selected from two sets:

\[
\alpha \in F_q^n \setminus \text{span}\{e_1, e_2, \ldots, e_k\} \tag{1}
\]

where \( \text{span}\{e_1, e_2, \ldots, e_k\} \) is the vector space that is span by the linearly independent vectors \( e_1, e_2, \ldots, e_k \):

\[
\alpha \in \text{span}\{e_1, e_2, \ldots, e_k\} \setminus \{c_1e_1 + c_2e_2 + \ldots + c_ke_k \mid c_1, c_2, \ldots, c_k \in F_q, 1 \leq i \leq k \} \tag{2}
\]

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 \( q^{(n-k)+k(p-1)} \) in (2).

Since \( A\xi_{i-1} = \xi_i, 2 \leq i \leq k \) and \( A\xi_k = \alpha = c_1e_1 + c_2e_2 + \ldots + c_ke_k \), \( A \) must have the following form:

\[
\begin{pmatrix}
\xi_1 \\
\vdots \\
0 & 1 & \cdots & 0 & c_{k-1} \\
0 & \cdots & 1 & c_1
\end{pmatrix}
\]

The characteristic polynomial of the matrix \( C_k \) is

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

\[
\begin{pmatrix}
C_k \\
D
\end{pmatrix}
\]

is the generalized orthormorphic matrix if and only if \( C_k, A_{n-k} \) is the generalized orthomorphic matrix by the definition of the generalized orthomrophic matrix on \( F_q \), so the characteristic roots of \( f(\lambda) = |\lambda I - C_k| \) can’t be 0, 1, …, \((p-1)\), that is:

\[
\begin{cases}
f(0) \neq 0 \\
f(1) \neq 0 \\
\vdots \\
f(p-1) \neq 0
\end{cases}
\]

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.

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

that requirement \( a_0, a_1, \ldots, a_{p-1} \) are all not 0.

\((a_0, a_1, \ldots, a_{p-1})^T\) Can be taken \((q-1)^p\) possible values, where \( c_1, c_2, \ldots, c_k \) 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 \((c_0, c_1, \ldots, c_k)^T\) given the value \((a_0, a_1, \ldots, a_{p-1})^T\), the value

\((c_0, c_1, \ldots, c_k)^T\) has \( q^{(k-p)} \) classes. Namely, the number of the generalized orthomorphic matrices formed \( C_k \) is \( q^{(k-p)} \).

The matrix \( D \) in \( A = \begin{pmatrix} C_k & D \\ 0 & A_{n-k} \end{pmatrix} \) has \( k \) rows and \( n-k \) columns, which has \( q^{(k-n)} \) classes. It will prove the opinion when \( \alpha \) fall in (2). If we denote:

\[
L_2(e_1, e_2, \ldots, e_k, \alpha) = \{ A \in L_n \mid A\xi_i = \xi_i, A\xi_k = \alpha, 2 \leq i \leq k \}
\]

then the number is:

\[
| L_2(e_1, e_2, \ldots, e_k, \alpha) | = q^{(n-k)+k-p} \cdot (q-1)^p \cdot | L_{n-k} |
\]

We have obtain the Recurrence relation:

\[
| L_n | = (q^* - q) \cdot | L_2(e_1, e_2) | 
\]

If \( k \geq 2 \) then

\[
L_2(e_1, e_2, \ldots, e_k, \alpha) = \bigcup_{\beta} L_2(e_1, e_2, \ldots, e_k, \beta)
\]

\( \bigcup_{\beta} L_2(e_1, e_2, \ldots, e_k, \beta) \) denotes that \( \alpha \) is taken from (1). Therefore, the counting formula is:

\[
| \bigcup_{\alpha} L_{n-k} e_1, e_2, \ldots, e_k, \alpha | =
\]

3076
\( (q^\alpha - q^1) | L_n(e_1, e_2, \cdots, e_k) | \)

\[ \bigcup_{\alpha} L_n(e_1, e_2, \cdots, e_k, \beta) \]

denotes that \( \alpha \) is taken from (2).

\[ | \bigcup_{\beta} L_n(e_1, e_2, \cdots, e_k, \beta) | = q^{k(n-k)+p}(q-1)^p | L_{n-k} | \]

Note \( L_n(e_1, e_2, \cdots, e_k, \cdots , e_k) = 0 \)

Summarily,

\[ | L_k | = \sum_{i, j} q^{(i-j)+k-p}(q-1)^j | L_{n-k} | (n, k \geq p) \]

we stipulate \( | L_0 | = 1, | L_1 | = 0 \) and \( | L_2, \cdots , L_{p-1} | \)

need to be calculated separately.

There are two advantages to calculate \( | L_2, \cdots , L_{p-1} | : \)

- 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 \( q = p = 2 \) then the counting formula of the \( n \) square orthomorphic matrices on \( F_2^n \) should be obtained.

The generalized orthomorphism on finite fields \( F_2^n \) can 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 \( f(x), f(x) + kX(1 \leq k \leq p - 1) \) 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 \( F(X), F(X) + kI(1 \leq k \leq p - 1) \) (1 is the identity) are the multi-output Boolean functions.

**Proposition 4:** Let \( S \) be a generalized orthomorphism on \( F_q^n \), if \( T \) is 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 \( f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \in F_q[x] \)

be an irreducible polynomial, the:

**\( n \times n \) Matrix**

\[
A = \begin{pmatrix}
0 & 0 & \cdots & 0 & -a_n \\
1 & 0 & \cdots & 0 & -a_{n-1} \\
0 & 1 & \cdots & 0 & -a_2 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & -a_1
\end{pmatrix}
\]

is said to be the companion matrix of \( f(x) \). In the application, the generalized linear orthomorphism on the finite field \( F_2^n \) 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 \( F_2^n \), which are as follows:

**Algorithm 1:**

**Step 1:** Find an irreducible polynomial \( f(x) \in F_2^n[x] \) of degree \( n \), or find a manic polynomial \( f(x) \in F_2^n[x] \) 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 \( F_2^n \) and carry on the similarity transformation \( C_f \) to \( AC_fA^{-1} \).
Step 4: Obtain the output \( A^T C A^{-1} \), 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 \( A^T C A^{-1} \) 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 \( F_q^2 \).

**Step 2:** Find an arbitrary matrix \( B \), make \( \begin{pmatrix} C & B \\ 0 & A \end{pmatrix} \) 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 \( P \begin{pmatrix} C & B \\ 0 & A \end{pmatrix} P^{-1} \).

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 \( F_q^2 \) 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 crypto logic components. It is the next major task that the generalized linear orthomorphisms on \( F_2^8 \) 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**


