Research Journal of Applied Sciences, Engineering and Technology 5(5): 1853-1858, 2013
DOI:10.19026/rjaset.5.4949
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: August 11, 2012 Accepted: September 03, 2012 Published: February 11, 2013

Research Article

The Properties of Orthomorphisms on the Galois Field

[1]Haiqing Han, [1]Xiaofang Xu 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: The orthomorphism on the Galois field is a kind of permutations that is the most widely used in cross-cutting issue, the orthomorphic polynomials over the finite field is an effective method to study it, this study has obtained the coefficients relationship of the orthomorphisms over the Galois field by algebraic methods. In addition, this study have understood the maximal subgroup structure and counting in the Abelian group. It is help to in-depth study the application and the nature of the orthomorphism qua the theoretical support.

Keywords: Orthomorphic polynomials, orthomorphisms, the domain of algebraic integer, the finite field, the maximal subgroup

INTRODUCTION

With the popularity of the computer and the Internet, the gate of the network is opening at the information age. Computer network and information security become more and more critical, the cryptography is one of the key technologies in information security. The permutation plays an important role in the cipher design; a well permutation can be used to design the cipher, the digital signature or authentication algorithms. In the cipher design, the cryptosystem based on mathematical hard problems has been usually divided into some cipher components to design, which these parts include the linear and nonlinear permutation. And the linear permutation is known as the P-permutation and the nonlinear permutation is called S-box (Haiqing and Huanguo, 2010). It is proved that the orthomorphisms have a good cryptographic property in Lohrop (1995): the complete balance. The orthomorphisms have been researched widely from the perspective of mathematics and cryptography and are also used in the design of the cipher, digital signature and authentication algorithms. The cryptosystem SMS4 is commercial block cipher in China whose round function is designed in the nonlinear orthomorphisms (Shuwang *et al*., 2008). In addition to the commercial cipher, there are other related applications to the orthomorphisms, including the research and development product DSD (Lohrop, 1995) enhanced security (Qibin and Cheng, 1996) and the construction of Boolean functions in cipher (Dawu *et al*., 1999).

In order to explore orthomorphisms on cryptographic properties and applications, people have studied the orthomorphisms from different perspectives:

- **The Latin square angle:** Latin square is used to study the orthomorphism over the Galois Field $GF(2^n)$ and which are obtained by the orthomorphic Latin square transversal in Baoyuan *et al*. (1997); in 2006, it is pointed out that there is the one to one corresponding relations between the orthomorphisms and the orthomorphic Latin square transversal (Shuwang *et al*., 2008), the counting bound of orthomorphisms have been obtained by the orthomorphic Latin square in Qi *et al*. (2008).
- **The permutation polynomials angle:** The permutation polynomials have been studied first the orthomorphisms over the Galois field in Zhihui (2002), including the distribution of permutation polynomials over $GF(2^2)$, $GF(2^3)$, $GF(2^4)$ and so on. The general conclusions have been obtained that a certain class of permutation polynomials do not exist in Yuan and Huanguo (2007), the degree distribution of the orthomorphic permutation polynomials on $GF(2^4)$ become clear through the classification method and the whole the orthomorphic permutation polynomials on $GF(2^4)$ are generated in Yuan and Huanguo (2007).
- **The boolean function angle:** Boolean functions have its own advantages in the construction and research to the permutation, (Dengguo and Zhenhua, 1996) have constructed some orthomorphisms over the Galois field using multi-

Corresponding Author: Xiaofang Xu, Department of Mathematics and Physics, Hubei Polytechnic University, Huangshi 435003, Hubei, China

output Boolean function, YANG Yixian and Gu Dawu etc., have also studied the orthomorphisms and obtained better results using the Boolean functions as the major weapons. It is more convenient to construct the orthomorphisms from low order to high order using the Boolean permutation method (Dengguo and Zhenhua, 1996; Dengguo and Zhenhua, 1998; and Yusen *et al*., 1999).

- **The loop structure angle of the permutation:** The Mathematical knowledge knows us that any permutation can be written in the product of circulated factors which does not intersect. The circulated factors are known as the circle structure. The circle structure has been used to study the circle structure characteristics of orthomorphisms (Dawu and Guozhen, 1997) and the maximum linear orthomorphisms (Zhihui, 2002; Anhua, 2003).
- **The angles of the vector representation and the permutation matrix:** Dr. L. Mittenthal and Xiao Guozhen have studies the orthomorphisms from the angles of the vector representation and the permutation matrix.

These different methods have their own advantages when the orthomorphisms are studied. If the example and enumeration of orthomorphisms need to be given, then it is more effective and convenient that we will utilize generally Latin square to carry on. If it needs to determine that the orthomorphism is linear or nonlinear, then we will use the multi-output Boolean permutation or permutation polynomial to judge it. When the maximum linear orthomorphisms are studied, we will use the circle structure of the permutation.

After the analysis of the domestic and international status of orthomorphisms, it is clear that the orthomorphisms are divided into the linear and non-linear from structural point of view. We have mainly studied the orthomorphisms issues including the structure, enumeration or counting upper and lower bounds. This study will study the relations of the orthomorphic permutation polynomial coefficients and the applications of the orthomorphisms in the maximal subgroups of the Galois field.

PRELIMINARIES

Let $F_2 = \{0, 1\}$ be a binary finite field. F_{2n} or $GF(2^n)$ = 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 be the finite field with an arbitrary prime number characteristic p, namely $q = p^k$. Similarly, F_q^n = The extension field of F_q with degree n. Let S be a bijection on $GF(2^n)$, that is satisfied:

- $\forall x, y \in GF(2^n)$ if $x \neq y$ then $S(x) \neq S(y)$
- For the arbitrary constant a, x is the existence and uniqueness, so that S(x) = a. We said S a permutation.

Definition 1: Let S be a permutation on GF (2^n), l be the identity transformation ($I(x) = x, \forall x \in GF(2^n)$). S is called an orthomorphism, if $S \oplus I$ is still a permutation on $GF(2^n)$ ($\oplus$ is the addition operation of $GF(2^n)$). Further, S = A linear orthomorphism on $GF(2^n)$, if S(X + Y) = S(X) + S(Y) set up $\forall X, Y \in GF(2^n)$.

By the definition 1, we have simply put the Galois field $GF(2^n)$ as an additive group when the orthomorphisms on the Galois field $GF(2^n)$ are studied. It has presented the existence theorem of the orthomorphisms in Hall and Paige (1957): the necessary and sufficient conditions that the orthomorphism exists in a finite Abelian group G are that the Sylow-2 subgroup of the group G is not cyclic group or is trivial.

It is indicated that a permutation is the orthomorphism if and only if the sum of the permutation and the identity transformation is still a permutation by Definition 1. The orthomorphisms is a special kind of the permutation and not all the permutations are the orthomorphisms.

Example 1: Let S be the permutation on $GF(2^2)$ and S satisfies:

$$(0,0) \mapsto (0,1), (0,1) \mapsto (1,0)$$

$$(1,0) \mapsto (0,0), (1,1) \mapsto (1,1)$$

then S is an orthomorphism. But the identity transformation on $GF(2^2)$ is not an orthomorphism.

Definition 2: Let G be a finite group, S be a bijection on G. If the mapping $S' : x \mapsto xS(x)$ is still the permutation on G, then S is called the complete mapping. (xS(x) represents the multiplication between x and S(x) in G).

Definition 3: Let G be a finite group, S be a bijection on G. If the mapping $S' : x \mapsto x^{-1}S(x)$ is still the permutation on G, then S is called the orthogonal mapping. ($x^{-1}S$ (x) = The multiplication between the inverse of x and S(x) in G).

Definition 4: Let S be a permutation on $GF(2^n)$, if V is an arbitrary maximal subgroup in $GF(2^n)$ (or a maximal subspace), and the complement set $\bar{V} = GF(2^n) \setminus V$ satisfies:

$$|S(V) \cap V| = |S(V) \cap \bar{V}| = 2^{n-2}$$

Then S is known as the perfectly balance mapping.

By the above definitions, the orthomorphism is the complete mapping, the orthogonal mapping and the perfectly balance mapping. The orthomorphisms have been well applied in practice because of its inherent cryptographic properties. We have first given the application of the orthomorphisms in the study of the maximal subgroups structure on the Galois Field GF(2^n).

RESULTS

The addition operation in the Galois field is denoted by $\oplus$, the Galois field is a group for the addition operation and you can study the maximal subgroups. At the same time, the Galois field can also be seen as an n-dimensional vector space, you can study the subspace. We have known that there is the one to one corresponding between the maximal subgroups and from the (n - 1) -dimension subspace limited nature of the domain and its maximal subgroups on GF(2^n) correspond to the dimension of subspace. It is easy to obtain the following results that we have researched the structure of maximal subgroups using the orthomorphism on GF(2^n).

Theorem 1: Let $\alpha_1, \alpha_{2,\ldots}, \alpha_n$ be a arbitrary basis of the Galois field GF(2^n) on F_2, taking out arbitrarily the (n - 1) vectors is spanning a subspace M on F_2, then M is a maximal subgroup on the addition operation on GF(2^n) and the all maximal subgroups on addition operation on GF(2^n) can be expressed as:

$$aM = \{am \mid m \in M\}, a \in GF(2^n) \setminus \{0\}$$

so there are (2^n - 1) maximal subgroups on GF(2^n).

Proof: Due to the Galois field GF(2^n) is a finite Abelian group for the addition operation, the order of the maximal subgroups on GF(2^n) is 2^{n-1} because of the cycle decomposition to the finite Abelian group. So the vector space M is a maximal subgroup on GF(2^n). From the algebra, $\forall x \in GF(2^n) \setminus \{0\}, N = \{0, x\}$ is a minimal group, There is a group isomorphism $M \cong GF(2^n)/N$. And there are the {2^n - 1} groups N = {0, x}, hence the number of the different maximal subgroups are (2^n - 1) on GF(2^n).

Next, we will give the evidence of the all maximal subgroups on GF(2^n) can be expressed as:

$$aM = \{am \mid m \in M\}, a \in GF(2^n) \setminus \{0\}$$

It is easy to understand by the definition of the group, if $a \in GF(2^n) \setminus \{0\}$ then $aM = \{am \mid m \in M\}$ is a subgroup on GF(2^n). We can judge that $aM = \{am \mid m \in M\}$ is a maximal subgroup by the order. For $a \in GF(2^n) \setminus \{0\}$, if $a = 1$ then $aM = \{am \mid m \in M\} = M$; if a ≠ 1 then f (x) = ax is being an orthomorphism on GF(2^n), the complete balance tells us M ≠ aM because the half elements of $f(M) = \{f(c) \mid c \in M\} = aM$ are in M and the other half are in $\bar{M} = GF(2^n) \setminus M$. At same reason, if $\forall a, b \in GF(2^n)/\{0\}$ and a ≠ b, then $ab^{-1}M \neq M \Leftrightarrow aM \neq bM$ and $aM = \{am \mid m \in M\}$ just has the (2^n - 1) non-zero elements. It goes to show when we have taken over all non-zero elements a in GF(2^n), $aM = \{am \mid m \in M\}$ is ergodic to the maximal subgroups on GF(2^n).

The orthomorphisms have a good effect on the study of algebraic structure as a special kind of mapping by the theorem 1. The orthomorphisms can also be used to the block design, statistical analysis, channel coding and the orthogonal Latin squares and so on. From the angle of the orthomorphic permutation polynomials to research the orthomorphisms in Zhihui (2002) and Yuan and Huanguo (2007), it is tells us that can study the orthomorphisms structure by the permutation polynomials. Let $F = GF(2^n), f \in F[X]$ be the polynomial, then $f(c) \in F$ for $\forall c \in F$. The polynomial f(X) is a transformation on GF(2^n). If f(X) is the one to one transformation, then f(X) is a permutation on GF(2^n), f(X) is called the permutation polynomial on GF(2^n). It has the following facts: that f(X) is the permutation polynomial on GF(2^n) is equivalent to one of the following conditions:

- $f : c \mapsto f(c)$ is injective on GF(2^n)
- f is a subjective on GF(2^n)
- $\forall a \in F$ the equation f(X) = a has solutions
- $\forall a \in F$ the equation f(X) = a has a unique solution

Definition 5: Let $f \in F_{2^n}[X]$ and f(X) = $a_0 + a_1 X + \ldots + a_n X^n$, if $a_n \neq 0$ the f(X) is said the polynomial of degree n, denoted deg (f(X)) = n.

Let S be a permutation on GF(2^n) and $S : c \mapsto S(c), \forall c \in GF(2^n)$, the corresponding permutation polynomial can be derived from the interpolation formula:

$$f(X) = \sum_{c \in GF(2^n)} S(c)(1-(x-c)^{q-1}) =$$

$$\sum_{c \in GF(2^n)} [S(c) \prod_{a \neq c} \frac{a-x}{a-c}], \text{ where } q = 2^n$$

f(X) is simplified to the degree deg (f(X)) ≤q - 1. It indicated that the arbitrary permutation can be used the polynomial with the degree is no more than (q - 1) to

represent. It is easy to know that if f(X) is the permutation polynomial on GF(2^n) then $GF(2^n)=\{f(c)\,|\,c\in GF(2^n)\}$, for $\gamma\in GF(2^n)$ satisfies $GF(2^n)=\{f(c)\oplus\gamma\,|\,c\in GF(2^n)\}$. It shows also that f(X) is the permutation on GF(2^n) if and only if $f(X)\oplus\gamma$ is the permutation on GF(2^n). Let $f(X)=a_0+a_1X+\cdots+a_{q-1}X^{q-1}$ be the permutation on GF(2^n) if and only if $f(X)+a_0=a_1X+\ldots+a_{q-1}X^{q-1}$ is the permutation on GF(2^n). So we can assume the constant is 0 overall.

If f(X) is the orthomorphic permutation polynomial, then the regular of coefficients is as follow:

Theorem 2: Let $f(X)=a_0+a_1X+\ldots+a_{q-1}X^{q-1}$ be an orthomorphic permutation polynomial on the Galois field GF(2^n), then the coefficients have the following relationships:

$$\sum_{i+i=q-1,i<j} a_ia_j=0 \text{ and } a_{q-2}+\sum_{i+i=q-1,i<j} a_ia_j=0$$

Proof: Let $q=2^n$, denoted GF(2^n) by F_q. A Galois field with the character 2 can be isomorphism to a residue class ring of the algebraic integer ring (Lang, 1994), namely it exists an algebraic integer ring E and its ideal 2E, such that $F_q\cong E/2E$. The isomorphic field is regarded as the same field, simply remember $F_q=E/2E$. It is very easy to get the natural ring homomorphism $\eta: E\to F_q=E/2E$ and ker η = 2E. The homomorphism can be lift to $\bar{\eta}: E[x]\to F_q[x]$ and the indeterminate met with $\bar{\eta}(x)=x$, the homomorphism $\bar{\eta}$ is restricted $\bar{\eta}|_E=\eta$ to E. Let g be the multiplication generator of the Galois field, the original image of g is e in E, we have the following relationship: $\bar{\eta}(e)=g$, $\bar{\eta}(e^{q-1})=g^{q-1}=1$, $\bar{\eta}(e^i)=g^i\neq 1, 1\le i<q-1$. There are exactly the q cossets of the algebraic integer ring E under its ideal 2E, the cosset decomposition of E is as follows E = {0+2E} $\cup_{i=01}^{q-1}(e^i+2E)$. And $\bar{\eta}(e^{q-1})=g^{q-1}=1=\bar{\eta}(1)$, so they are belong to the same cosset between 1 and e^{q-1}. Hence, $(e^{q-1}-1)\in 2E$, that is $e^{q-1}=1 \pmod 2$.

Similarly, $e^i=0 \pmod 2$, $1\le i<q-1$ (if $e^i=1 \pmod 2$), $1\le i<q-1$, we can get $\bar{\eta}(e^i)=g^i=1(1\le i<q-1)$, which is the contradiction to the multiplication generator g)

Next, we have proved that $e^{q-1}=1 \pmod 4$, if $e^{q-1}=0 \pmod 4\neq 1$, then:

$$[e(1+2(\frac{e^{q-1}-1}{2})]^{q-1}=$$

$$e^{q-1}+C_{q-1}^1e^{q-1-1}2e\frac{e^{q-1}-1}{2}+\sum_{i=2}^{q-1}C_{q-1}^ie^{q-1-i}[2e\frac{e^{q-1}-1}{2}]^i$$

$$= e^{q-1}+2(q-1)e^{q-1}\frac{e^{q-1}-1}{2}(\mathrm{mod}\,4)$$

$$= e^{2(q-1)}(\mathrm{mod}\,4)$$

$$= 1+(e^{q-1}-1)\cdot 2\frac{e^{q-1}-1}{2}(\mathrm{mod}\,4)$$

$$= 1 \pmod 4$$

(where $4\,|e^{q-1}-1$)

Owing also to $\bar{\eta}([e\left(1+2\left(\frac{e^{q-1}-1}{2}\right)\right)]^{q-1})=\bar{\eta}(e^q)=g^q=\bar{\eta}(e)=g$, it is indicated that e^q and e are in the same cosset and the representative element in the cosset can be select randomly, so we can select $e'=e^q$ as the representative element to satisfy:
$(e')^{q-1}\equiv 1(\mathrm{mod}\,4)$, without loss of generality:

$$e^{q-1}=1 \pmod 4 \quad (1)$$

Let $S=\{0,e^i\,|\,0\le i\le q-1\}\subset E$, it is obvious to $\{\bar{\eta}(x)\,|\,x\in S\}=F_q$. The power sum of the elements has the following relationship:

$$\sum_{x\in S}x^t=\begin{cases}3(mod\,4) & (q-1)\,|\,t\\ 0(\mathrm{mod}\,4) & (q-1)\nmid t\end{cases} \quad (2)$$

Because of:

$$\sum_{x\in S}x^t=\sum_{i=0}^{q-1}(e^t)^i=1+e^t+(e^t)^2+\cdots+(e^t)^{q-2}=\frac{(e^t)^{q-1}-1}{e^t-1}$$

if $(q-1)|\,t$, then the above equation is:

$$\sum_{x\in S}x^t=1+e^t+(e^t)^2+\cdots+(e^t)^{q-2}=q-1=2^n-1=3(\mathrm{mod}\,4)$$

if $(q-1)|\,t$, then the above equation is:

$$\sum_{x\in S}x^t=\sum_{i=0}^{q-1}(e^t)^i=\frac{(e^t)^{q-1}-1}{e^t-1}$$

Due to $e^t\not\equiv 1(\mathrm{mod}\,2)$, $1\le t\le q-1$, if t is the odd, since $4|\,(e^{q-1}-1)$ and $(e^t)^{q-1}-1=(e^{q-1})^t-1$, then $4|\,((e^{q-1})^t-1)$ that is $4\,|[\frac{(e^{q-1})^t-1}{e^t-1}]$; If t is the event, then $(e^{2(q-1)}-1)\,|\,((e^{(q-1)t}-1))$, in addition to $4|(e^{q-1}-1)$, so $2|(e^{q-1}-1)$, that is $2|(e^{q-1}+1)$. Hence $8\,|\,(e^{2(q-1)}-1)$, $(e^{2(q-1)}-1)$, $((e^{q-1})^t-1)$, That is $8\,|\,((e^{q-1})^t-1)$. But

$e^t \not\equiv 1 (\mathrm{mod}\, 2)$, we have the equation $4 \mid [\frac{(e^{q-1})^t - 1}{e^t - 1}]$.

Assume:

$$F(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{q-1} x^{q-1} \in E[x]$$
$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{q-1} x^{q-1} \in F_q[x]$$

and,

$$\bar{\eta}(F(x)) = f(x)$$

Because f(x) is a permutation, so $\{\bar{\eta}(F(x))|x \epsilon S\} = \{f(0), f(g^i)|0 \le i \le q-2\} = F_q \ \forall x \epsilon S, \sum_{x \epsilon S} F^2(x) =$ *x∈S(x+2y)2, y∈E, = x∈Sx2(mod4)* (by the definition of the cosset) = 0(mod 4) (by the Eq. (2) On the other hand:

$$\sum_{x \in S} F^2(x) = \sum_{x \in S} (\sum_{i=0}^{q-1} b_i x^i)^2 = \sum_{x \in S} (\sum_{i=0}^{q-1} b_i^2 x^{2i}) + \sum_{x \in S} \sum_{i<j} 2 b_i b_j x^{i+j}$$

$$= \sum_{i=0}^{q-1} b_i^2 \sum_{x \in S} x^{2i} + \sum_{i<j} 2 b_i b_j \sum_{x \in S} x^{i+j}$$

By (2) and 2i | (q - 1), the above equation satisfies:

$$\sum_{x \in S} F^2(x) = \sum_{x \in S} (\sum_{i=0}^{q-1} b_i x^i)^2 = \sum_{i+j=q-1, i<j} 2 b_i b_j (\mathrm{mod}\, 4)$$

So,

$$0 = \sum_{i+j=q-1, i<j} 2 b_i b_j (\mathrm{mod}\, 4)$$

From the nature of the congruence:

$$0 = \sum_{i+j=q-1, i<j} b_i b_j (\mathrm{mod}\, 2) \Rightarrow (\sum_{i+j=q-1, i<j} b_i b_j) \in 2E = \ker \bar{\eta} = \ker \eta$$

So,

$$\sum_{i+j=q-1, i<j} a_i a_j = \bar{\eta}(\sum_{i+j=q-1, i<j} b_i b_j) = 0$$

If f(x) is an orthomorphism, so is f(x) + x, then its coefficient must also satisfy the above property. The second equation in the theorem is the coefficients relationship of f(x) + x, it must be established. The theorem has been proved.

For the orthomorphic permutation polynomials, the polynomials of degree (q - 2) must not exist (Daqing, 1986). It is necessary to $a_{q-2} = 0$, the two formulas in the theorem are equivalent. We can also get more information on the relationship to the coefficients in the orthomorphic permutation polynomial, which needs further study.

The proof of theorem 2 has only used the map $\bar{\eta}(F(x)) = f(x)$ and the square relationships between the original image and the image. We can further research the cubed, the fourth power relationships between the original image and the image and so on. We can get more relationship on the coefficients of the orthomorphic permutation polynomial. These related equations reveal that the coefficients of the orthomorphic permutation polynomials exist in the constraint relations. If this research is clear, then it can help us to obtain the counting formula of the orthomorphisms by solving the equation system.

CONCLUSION

This study has mainly studied the properties of the orthomorphisms over the Galois field GF(2^n). Theorem 1 tells us, the orthomorphisms are a special kind of mappings, such as isomorphism and homomorphism, which has an unexpected effect to study the algebraic structure itself. It is mainly to study the coefficients relationships of the orthomorphisms in Theorem 2. The coefficients of the orthomorphisms must have the restrictive relationships as a special kind of permutation polynomial. It is an important way to study counting formula of the orthomorphisms that such constraint relationships are search for. All in all, if we want to get more conclusions on the orthomorphisms on the Galois field, their applications and structure need further study.

ACKNOWLEDGMENT

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

REFERENCES

Anhua, Z., 2003. The research and construction of orthomorphic permutation. MA Thesis, National University of Defense Techology, Changsha.

Baoyuan, K., T. Jianbo and W. Yumin, 1997. Two results about orthomorphic permutation and orthomorphic latin square. J. XiDian Univ., 24: 421-424.

Daqing, W., 1986. On a problem of niederreiter and robinson about finite fields. J. Astrual. Math. Soc. Ser A, 41: 336-338.

Dawu, G. and X. Guozhen, 1997. An improved method of constructing nonlinear orthomorphic permutation with the analysis of its property. J. XiDian Univ., 24: 477-481.

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

Dengguo, F. and L. Zhenhua, 1996. On the construction of the orthomorphic permutation. Secure Commun., 2: 61-64.

Dengguo, F. and L. Zhenhua, 1998. An iterated method of constructing orthomorphic permutation. Secure Commun., 2: 53-54.

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

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

Lang, S., 1994. Algebraic Number Theory [M]. 2nd Edn., GTM110, Springer-Verlag, New York.

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

Qi, L., Z. Yin, C. Cheng and L. Shuwang, 2008. Construction and counting orthomorphism based on transversal. International Conference on Computational Intelligence and Security, Suzhou, China.

Qibin, Z. and Z. Ken Cheng, 1996. On transformations with halving effect on certain subvarieties of the space Vm (F2). Proceedings of China Crypt', Zhengzhou.

Shuwang, L., F. Xiubin, *et al*., 2008. Complete Mapping and Application in Cryptography. China University of Technology Press, Hefei, China.

Yuan, Y. and Z. Huanguo, 2007. A note on orthomorphic permutation polynomial. J. Wuhan Univ. Nat. Sci., 53: 33-36.

Yusen, X., L. Xiaodong, Y. Yixian and Y. Fangchun, 1999. Constructions and enumerations of orthomorphic permutations in cryptosystems. J. Inst. Commun., 20: 27-30.

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