A Note on the Constructions of Orthomorphic Permutations

Jianqin Zhou
Telecommunication School, Hangzhou Dianzi University, Hangzhou 310018, China
Department of Computer Science, Anhui University of Technology, Ma'anshan 243002, China
(Email: zhou@hdu.edu.cn)

(Received Sept. 15, 2007; revised and accepted May 9, 2008)

Abstract

Orthomorphic permutations have important applications in the design of block ciphers. A practical algorithm is derived to generate all orthomorphic permutations over F_2^m, and it is verified that the number of all orthomorphic permutations over F_2^4 is 244,744,192. With the theory of finite fields, a brief method is derived to generate a permutation polynomial corresponding to every permutation over F_2^m, and all orthomorphic permutation polynomials over F_2^4 are analyzed.

Keywords: Block cipher, orthomorphic permutation, polynomial

1 Introduction

Block ciphers are widely used in cryptology and Internet communications. Constructing new block ciphers which are resistant to cryptanalysis has attracted the attention of researchers for the past twenty years. Orthomorphisms have important applications in the design of block ciphers [5], and have a strong relationship to the design of hashing functions and pseudo-random sequence generators.

Let $S^o(m)$ denote the set of orthomorphic permutations of order 2^m, Liu and Shu in [4] proposed a method to generate orthomorphic permutations of high order randomly by recursively combining small orthomorphic permutations, and proved that $|S^o(m)| > 2^{2^m}$.

With the polynomial theory in finite fields, orthomorphic permutation polynomials over finite field F_2^3 is discussed, and the detailed expressions and the enumeration of orthomorphic permutation polynomials over F_2^3 is obtained [1, 2].

In this note, a practical algorithm is derived to generate all orthomorphic permutations over F_2^m, and it is verified that the number of all orthomorphic permutations over F_2^4 is 244,744,192. With the theory of finite fields, a brief method is derived to generate a permutation polynomial corresponding to every permutation over F_2^m, and all orthomorphic permutation polynomials over F_2^4 are analyzed.

We first introduce some definitions and lemmas, which can be found in [1, 2].

Throughout this paper, finite field F_q is occasionally denoted by F_p^m or $GF(p)^m$, where $q = p^m$, p is a positive prime number, $GF(p) = \{0, 1, 2, \cdots, p-1\}$.

Definition 1. *A permutation σ on F_2^m is called an orthomorphic permutation if $x \mapsto x \oplus \sigma(x), \forall x \in F_2^m$, is also a permutation, where $\bigoplus$ stands for bit wise addition modulo 2.*

We identify an $m-$bit binary vector $(a_0, a_1, \cdots, a_{m-1})$ with an integer $i = \sum_{j=0}^{m-1} a_j 2^j$. Thus a permutation P can be represented as,

$$P = \begin{pmatrix} 0 & 1 & 2 & \cdots & n-1 \\ \sigma(0) & \sigma(1) & \sigma(2) & \cdots & \sigma(n-1) \end{pmatrix},$$

where $\sigma(i) \in F_2^m, 0 \leq i < n, n = 2^m$. It can be abbreviated as,

$$P = \{\sigma(0), \sigma(1), \sigma(2), \cdots, \sigma(n-1)\}.$$

An identical permutation is denoted as,

$$I = \{0, 1, 2, \cdots, n-1\}.$$

For $m = 2$, as $\{2 \bigoplus 0, 1 \bigoplus 1, 3 \bigoplus 2, 0 \bigoplus 3\} = \{2, 0, 1, 3\}$, both {2,1,3,0 } and {2,0,1,3 } are orthomorphic permutations.

Definition 2. *A function $f : F_2^m \to F_2^m$ is said to be a permutation polynomial, if $f \in F_q[x]$ and f is a one-to-one mapping, where $q = 2^m$.*

Definition 3. *A function $f : F_2^m \to F_2^m$ is called an orthomorphic permutation polynomial if both $f(x)$ and $x \oplus f(x)$ over F_2^m are permutation polynomials.*

It is well known that any function $f : F_2^m \to F_2^m$ can be represented by a polynomial $F \in F_q[x]$ with an order less than $q = 2^m$. Hence we only need to consider the permutation polynomials of order less than $q = 2^m$.

Lemma 1. *If both function $f : F_2^m \to F_2^m$ and function $g : F_2^m \to F_2^m$ are permutation polynomials, then function $f \diamond g : F_2^m \to F_2^m$ is a permutation polynomial, where $f \diamond g(x) = f(g(x))$ for every $x \in F_2^m$.*

Note that for any constant $r \in F_2^m, x + r$ is a permutation polynomial, the following Lemma 2 and Lemma 3 are immediate.

Lemma 2. *$f(x) \in F_q[x]$ is a permutation polynomial if and only if for every $r \in F_q$, $f(x) + r$ is a permutation polynomial.*

Lemma 3. *$f(x) \in F_q[x]$ is an orthomorphic permutation polynomial if and only if for every $r \in F_q$, $f(x) + r$ is an orthomorphic permutation polynomial.*

Lemma 4. *$f(x) = ax + b \in F_q[x]$ is an orthomorphic permutation polynomial if and only if $a \neq 0, 1$.*

Let $F_q = Z_p(y)/g(y)$, where $g(y)$ is a irreducible polynomial, and $\deg(g(y)) = m$, p is a prime. Then F_q is a finite field with character $p, q = p^m$.

Let $h : b_0 + b_1 y + \cdots + b_{m-1} y^{m-1} \mapsto (b_0, b_1, \cdots, b_{m-1})$, where $b_i \in GF(p)$. Then h is a natural isomorph from F_q to F_p^m.

The following lemmas are the main results of [1].

Lemma 5. *Let $h : b_0 + b_1 y + \cdots + b_{m-1} y^{m-1} \mapsto (b_0, b_1, \cdots, b_{m-1})$, where $b_i \in GF(p)$. Let σ be a permutation over F_p^m, $f(x) = h^{-1}\sigma h$. Then $f(x) \in F_q[x]$ is a permutation polynomial, where $deg(f(x)) < q, q = p^m$. On the contrary, let $f(x) \in F_q[x]$ be a permutation polynomial, $\sigma = hf(x)h^{-1}$. Then σ is a permutation over F_p^m.*

Lemma 6. *Let σ be a permutation over F_p^m, $f(x) = h^{-1}\sigma h$. Then σ is an orthomorphic permutation if and only if $f(x) \in F_q[x]$ is an orthomorphic permutation polynomial, where $deg(f(x)) < q, q = p^m$.*

Thus, the enumeration of orthomorphic permutations over F_p^m is equivalent to the enumeration of orthomorphic permutation polynomials over $F_q, q = p^m$.

2 An Algorithm to Construct Orthomorphic Permutations

Let σ be an orthomorphic permutation over F_2^m. From Lemma 3, $\tau = \sigma + \sigma(0)$ is also an orthomorphic permutation over F_2^m and $\tau(0) = 0$, hence we only need to consider the orthomorphic permutation σ such that $\sigma(0) = 0$.

In fact, for every orthomorphic permutation σ, there exists a point α, such that $\sigma(\alpha) = \alpha$. As $\sigma + I$ is a permutation, where I is an identical permutation, hence there exists a point α, such that $\sigma(\alpha) + \alpha = 0$, namely, $\sigma(\alpha) = \alpha$.

We now consider the orthomorphic permutation a over $\{0, 1, 2, \cdots, n-1\}$, where $n = 2^m$. The permutation a is represented as $\{a[0], a[1], a[2], \cdots, a[n-1]\}$. The main idea of the algorithm is as follows.

We select $a[k]$, so that $a[k]$ is not equal to any of $a[0], a[1], a[2], \cdots, a[k-1]$, and $a[k] \oplus k$ is not equal to any of $a[0] \oplus 0, a[1] \oplus 1, a[2] \oplus 2, \cdots, a[k-1] \oplus (k-1)$.

Algorithm 1. To construct an orthomorphic permutation.

```
// global variables
char num[n];
/*here we consider orthomorphic permutations over
{0, 1, 2, ··· , n − 1} */
char conflag;
/* Suppose we have selected numc+1 integers,
num[0],num[1],···,num[numc]. In the array bixor,
the values with indexes num[0]⊕0,num[1]⊕1, ···,
num[numc-1]⊕(numc-1), respectively, are all set to
1, otherwise set to 0. num[0]⊕0,num[1]⊕1, ···,
num[numc]⊕(numc) are distinct integers. */
void ortho(int numc,char *bitxor)
{
  char select[n];
  char i,j,k;
  char bitxorn[n];
  i=0;
  //loop to find the n-(numc+1) unselected integers
  //from {0, 1, 2, ··· , n − 1}.
  for(j=0; j< n; j++)
  {
    conflag=0;
    for(k=0;k<numc+1;k++)
      if(j==num[k]){conflag=1;break;}
    if(conflag)continue;
    //j is one of the unselected integer.
    if(numc< n-2)
    {
      select[i]=j;
      i++;
    }
    else
    {
      if(bitxor[j⊕(n-1)]==1)return;
      if(j⊕(n-1)==num[numc]⊕numc)return;
      //Output the orthomorphic permutations.
      for(i=0;i< n-1;i++)printf(" %d",num[i]);
      printf(" %d ",j);
      return;
    }
  }
  // select num[numc+1] from select[].
  for(i=0;i< n;i++)bitxorn[i]=bitxor[i];
  bitxorn[num[numc]⊕numc]=1;
  for (j=0;j< n-1-numc;j++)
  {
    if(bitxorn[select[j]⊕(numc+1)]==1)continue;
    num[numc+1]=select[j];
    /* here we can not change
    bitxorn[select[j]⊕(numc+1)].*/
    ortho(numc+1,bitxorn);
```

```
    }
}
```

As we only need to consider the orthomorphic permutation σ such that $\sigma(0) = 0$, we can call the function ortho() like the following to find all orthomorphic permutations over {0,1,2,$\cdots$,n-1 }.

```
num[0]=0;
for(i=0;i< n;i++)bitxor[i]=0;
ortho(0,bitxor);
```

For $n = 16$, we have made a test by a computer with CPU Celeron 2.0G. It takes 6 minutes to find all 15,296,512 orthomorphic permutations σ over {0,1,2,$\cdots$, 14, 15 } such that $\sigma(0) = 0$. Thus the number of all orthomorphic permutations over F_2^4 is $15,296,512 \times 16 = 244,744,192$.

For $n = 32$, setting the first 14 integers of orthomorphic permutations over {0,1,2,$\cdots$,n-1 } be {0,2,4,6,3,1,7,5,16,18,20,22,19,17}, respectively, we found 2,375,680 orthomorphic permutations by calling function ortho().

3 A Method to Construct Permutation Polynomials

We now consider a method to construct permutation polynomials corresponding to the permutations over F_2^m. Here $\cdot$ denotes the multiplication over F_2^m, and both + and - denote the addition over F_2^m.

Let F_2^m be a finite field. It is well known that $F_2^m - \{0\}$ is a multiplication cyclic group of order $2^m - 1$. Let u be the generator of $F_2^m - \{0\}, q = 2^m$. Then $F_2^m = \{0, 1, u, u^2, \cdots , u^{q-2}\}$.

Let $f(y) = a_0 + a_1y + a_2y^2 + \cdots + a_{q-1}y^{q-1}$, where $a_i \in F_2^m, 0 \le i < q$, correspond to an orthomorphic permutation $\{p[0], p[1], p[u], p[u^2], \cdots , p[u^{q-2}]\}$. We assume $a_0 = 0$ since we only consider the orthomorphic permutation p such that $p[0] = 0$.

In other words, we want $a_1, a_2, \cdots , a_{q-1}$ to satisfy the following equation array.

$$\left\{\begin{array}{ll} a_1 \cdot 1 + a_2 \cdot 1^2 + & \\ \quad \cdots + a_{q-1} \cdot 1^{q-1} & = p[1], \\ a_1 \cdot u^1 + a_2 \cdot (u^1)^2 + & \\ \quad \cdots + a_{q-1} \cdot (u^1)^{q-1} & = p[u^1], \\ a_1 \cdot u^2 + a_2 \cdot (u^2)^2 + & \\ \quad \cdots + a_{q-1} \cdot (u^2)^{q-1} & = p[u^2] \\ \quad \cdots\cdots\cdots & \\ a_1 \cdot u^{q-2} + a_2 \cdot (u^{q-2})^2 + & \\ \quad \cdots + a_{q-1} \cdot (u^{q-2})^{q-1} & = p[u^{q-2}]. \end{array}\right. \quad (1)$$

We rewrite Equation (1) as the following.

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ u & u^2 & u^3 & \cdots & u^{q-1} \\ (u^2) & (u^2)^2 & (u^2)^3 & \cdots & (u^2)^{q-1} \\ & \cdots\cdots & & & \\ (u^{q-2}) & (u^{q-2})^2 & (u^{q-2})^3 & \cdots & (u^{q-2})^{q-1} \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_{q-1} \end{pmatrix} = \begin{pmatrix} p[1] \\ p[u] \\ p[u^2] \\ \vdots \\ p[u^{q-2}] \end{pmatrix}$$

Note that 1=1+1+1 and $1 + u^i + (u^2)^i + \cdots + (u^{q-2})^i = \frac{(u^i)^{q-1}-1}{u^i-1} = 0$, where i is a positive integer and $i \ne 0($ mod $(q-1))$. It is easy to show that the following identity holds.

$$\begin{pmatrix} 1 & (u)^{q-2} & (u^2)^{q-2} & \cdots & (u^{q-2})^{q-2} \\ 1 & (u)^{q-3} & (u^2)^{q-3} & \cdots & (u^{q-2})^{q-3} \\ 1 & (u)^{q-4} & (u^2)^{q-4} & \cdots & (u^{q-2})^{q-4} \\ & & \cdots\cdots & & \\ 1 & 1 & 1 & \cdots & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & \cdots & 1 \\ u & u^2 & \cdots & u^{q-1} \\ (u^2) & (u^2)^2 & \cdots & (u^2)^{q-1} \\ & \cdots\cdots & & \\ (u^{q-2}) & (u^{q-2})^2 & \cdots & (u^{q-2})^{q-1} \end{pmatrix} = I,$$

where I is an identity matrix. Then we have,

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_{q-1} \end{pmatrix} = \begin{pmatrix} 1 & (u)^{q-2} & \cdots & (u^{q-2})^{q-2} \\ 1 & (u)^{q-3} & \cdots & (u^{q-2})^{q-3} \\ 1 & (u)^{q-4} & \cdots & (u^{q-2})^{q-4} \\ & & \cdots\cdots & \\ 1 & 1 & \cdots & 1 \end{pmatrix} \cdot \begin{pmatrix} p[1] \\ p[u] \\ p[u^2] \\ \vdots \\ p[u^{q-2}] \end{pmatrix} \quad (2)$$

From Identity (2), we obtain, the following theorem.

Theorem 1. *Let $F_2^m = \{0, 1, u, u^2, \cdots u^{q-2}\}$, $\{a[0], a[1], a[u], a[u^2], \cdots a[u^{q-2}]\}$ be a transform over $\{0, 1, u, u^2, \cdots u^{q-2}\}$, where $q = 2^m$. Let $p[u^i] = a[u^i] - a[0], 1 \le i < q, f(y) = a_0 + a_1y + a_2y^2 + a_3y^3 + \cdots + a_{q-1}y^{q-1}$, where $a_0 = a[0], a_i, 1 \le i < q$, is defined by Identity (2). Then $f(0) = a[0]$, and $f[u^i] = a[u^i], 1 \le i < q$.*

Theorem 1 is a generalization of Lemma 5, which is the main result of [1].

Let $\{a[0], a[1], a[u], a[u^2], \cdots , a[u^{q-2}]\}$ be a permutation over $\{0, 1, u, u^2, \cdots , u^{q-2}\}$. Let $p[u^i] = a[u^i] -$

$a[0], 1 \leq i < q$. Then $\{p[1], p[u], p[u^2], \cdots, p[u^{q-2}]$ is a permutation over $\{1, u, u^2, \cdots u^{q-2}\}$. Note that $1 + u + u^2 + \cdots + u^{q-2} = 0$, from Identity (2), the following Theorem 2 is immediate.

Theorem 2. *Let $f(y) = a_0 + a_1 y + a_2 y^2 + a_3 y^3 + \cdots + a_{q-1} y^{q-1}$ be a permutation polynomial over $F_2^m = \{0, 1, u, u^2, \cdots u^{q-2}\}$, where $q = 2^m$. Then $a_{q-1} = 0$, namely, $deg(f(y)) \leq q - 2$.*

Let $GF(8) = \{0, 1, x, 1+x, x^2, 1+x^2, x+x^2, 1+x+x^2\}$. It is easy to show that $GF(8)$ is a finite field with multiplication modulo $x^3 + x + 1$. Let 2,3,4,5,6,7 denote $x, 1+x, x^2, 1+x^2, x+x^2, 1+x+x^2$, respectively. Then the all possible multiplications over $GF(8)$ can be listed as the following.

$$(m_{ij})_{8\times 8} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 2 & 4 & 6 & 3 & 1 & 7 & 5 \\ 0 & 3 & 6 & 5 & 7 & 4 & 1 & 2 \\ 0 & 4 & 3 & 7 & 6 & 2 & 5 & 1 \\ 0 & 5 & 1 & 4 & 2 & 7 & 3 & 6 \\ 0 & 6 & 7 & 1 & 5 & 3 & 2 & 4 \\ 0 & 7 & 5 & 2 & 1 & 6 & 4 & 3 \end{pmatrix}$$

Here m_{ij}, $0 \leq i < 8, 0 \leq j < 8$, stands for the multiplication of $i \in GF(8)$ and $j \in GF(8)$ modulo $x^3 + x + 1$.

It is easy to show that any of 2,3,4,5,6,7 can be the generator of $GF(8) - \{0\}$. Take 2 as an example, $2^2 = 4$, $2^3 = 3$, $2^4 = 6$, $2^5 = 7$, $2^6 = 5$, $2^7 = 1$.

Let $f(y) = a_0 + a_1 y + a_2 y^2 + a_3 y^3 + a_4 y^4 + a_5 y^5 + a_6 y^6 + a_7 y^7$, where $a_i \in GF(8), 0 \leq i \leq 7$, correspond to an orthomorphic permutation $\{p[0], p[1], p[2], \cdots, p[7]\}$. We assume $a_0 = 0$ since we only consider the orthomorphic permutation p such that $p(0) = 0$.

In other words, we want $a_1, a_2, a_3, a_4, a_5, a_6, a_7$ to satisfy the following equation array.

$$\begin{cases} a_1 \cdot 1 + a_2 \cdot 1^2 + a_3 \cdot 1^3 \\ +a_4 \cdot 1^4 + a_5 \cdot 1^5 + a_6 \cdot 1^6 + a_7 \cdot 1^7 = p[1], \\ a_1 \cdot 2 + a_2 \cdot 2^2 + a_3 \cdot 2^3 \\ +a_4 \cdot 2^4 + a_5 \cdot 2^5 + a_6 \cdot 2^6 + a_7 \cdot 2^7 = p[2], \\ a_1 \cdot 4 + a_2 \cdot 4^2 + a_3 \cdot 4^3 \\ +a_4 \cdot 4^4 + a_5 \cdot 4^5 + a_6 \cdot 4^6 + a_7 \cdot 4^7 = p[4], \\ a_1 \cdot 3 + a_2 \cdot 3^2 + a_3 \cdot 3^3 \\ +a_4 \cdot 3^4 + a_5 \cdot 3^5 + a_6 \cdot 3^6 + a_7 \cdot 3^7 = p[3], \\ a_1 \cdot 6 + a_2 \cdot 6^2 + a_3 \cdot 6^3 \\ +a_4 \cdot 6^4 + a_5 \cdot 6^5 + a_6 \cdot 6^6 + a_7 \cdot 6^7 = p[6], \\ a_1 \cdot 7 + a_2 \cdot 7^2 + a_3 \cdot 7^3 \\ +a_4 \cdot 7^4 + a_5 \cdot 7^5 + a_6 \cdot 7^6 + a_7 \cdot 7^7 = p[7], \\ a_1 \cdot 5 + a_2 \cdot 5^2 + a_3 \cdot 5^3 \\ +a_4 \cdot 5^4 + a_5 \cdot 5^5 + a_6 \cdot 5^6 + a_7 \cdot 5^7 = p[5]. \end{cases}$$

Let $u = 2, q = 8$. From Identity (2), we obtain,

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 7 & 6 & 3 & 4 & 2 \\ 1 & 7 & 3 & 2 & 5 & 6 & 4 \\ 1 & 6 & 2 & 7 & 4 & 5 & 3 \\ 1 & 3 & 5 & 4 & 7 & 2 & 6 \\ 1 & 4 & 6 & 5 & 2 & 3 & 7 \\ 1 & 2 & 4 & 3 & 6 & 7 & 5 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} p[1] \\ p[2] \\ p[4] \\ p[3] \\ p[6] \\ p[7] \\ p[5] \end{pmatrix} \quad (3)$$

From Identity (3), we have obtained by computer the detailed expressions and the enumeration of all $48 \times 8 = 384$ orthomorphic permutation polynomials over $GF(8)$. We have verified that if $f(y) = a_0 + a_1 y + a_2 y^2 + a_3 y^3 + a_4 y^4 + a_5 y^5 + a_6 y^6 + a_7 y^7$ is an orthomorphic permutation polynomial over $GF(8)$, then $a_3 = a_5 = a_6 = a_7 = 0$.

In a similar way to the above argument, we now consider orthomorphic permutation polynomials over $GF(16)$.

Let $GF(16) = \{0, 1, x, 1+x, x^2, 1+x^2, x+x^2, 1+x+x^2, x^3, 1+x^3, x+x^3, 1+x+x^3, x^2+x^3, 1+x^2+x^3, x+x^2+x^3, 1+x+x^2+x^3\}$. It is easy to show that with multiplication modulo $x^4 + x + 1$, $GF(16)$ is a finite field. Let 2,3,4,5,6,7,8,9,10,11,12,13,14,15 denote $x, 1+x, x^2, 1+x^2, x+x^2, 1+x+x^2, x^3, 1+x^3, x+x^3, 1+x+x^3, x^2+x^3, 1+x^2+x^3, x+x^2+x^3, 1+x+x^2+x^3$, respectively. Then the all possible multiplications over $GF(16)$ can be listed as the following.

$$(m_{ij})_{16\times 16} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 0 & 2 & 4 & 6 & 8 & 10 & 12 & 14 & 3 & 1 & 7 & 5 & 11 & 9 & 15 & 13 \\ 0 & 3 & 6 & 5 & 12 & 15 & 10 & 9 & 11 & 8 & 13 & 14 & 7 & 4 & 1 & 2 \\ 0 & 4 & 8 & 12 & 3 & 7 & 11 & 15 & 6 & 2 & 14 & 10 & 5 & 1 & 13 & 9 \\ 0 & 5 & 10 & 15 & 7 & 2 & 13 & 8 & 14 & 11 & 4 & 1 & 9 & 12 & 3 & 6 \\ 0 & 6 & 12 & 10 & 11 & 13 & 7 & 1 & 5 & 3 & 9 & 15 & 14 & 8 & 2 & 4 \\ 0 & 7 & 14 & 9 & 15 & 8 & 1 & 6 & 13 & 10 & 3 & 4 & 2 & 5 & 12 & 11 \\ 0 & 8 & 3 & 11 & 6 & 14 & 5 & 13 & 12 & 4 & 15 & 7 & 10 & 2 & 9 & 1 \\ 0 & 9 & 1 & 8 & 2 & 11 & 3 & 10 & 4 & 13 & 5 & 12 & 6 & 15 & 7 & 14 \\ 0 & 10 & 7 & 13 & 14 & 4 & 9 & 3 & 15 & 5 & 8 & 2 & 1 & 11 & 6 & 12 \\ 0 & 11 & 5 & 14 & 10 & 1 & 15 & 4 & 7 & 12 & 2 & 9 & 13 & 6 & 8 & 3 \\ 0 & 12 & 11 & 7 & 5 & 9 & 14 & 2 & 10 & 6 & 1 & 13 & 15 & 3 & 4 & 8 \\ 0 & 13 & 9 & 4 & 1 & 12 & 8 & 5 & 2 & 15 & 11 & 6 & 3 & 14 & 10 & 7 \\ 0 & 14 & 15 & 1 & 13 & 3 & 2 & 12 & 9 & 7 & 6 & 8 & 4 & 10 & 11 & 5 \\ 0 & 15 & 13 & 2 & 9 & 6 & 4 & 11 & 1 & 14 & 12 & 3 & 8 & 7 & 5 & 10 \end{pmatrix}$$

Here m_{ij}, $0 \leq i < 16, 0 \leq j < 16$, stands for the multiplication of $i \in GF(16)$ and $j \in GF(16)$ modulo $x^4 + x + 1$.

From Identity (2) and $(m_{ij})_{16\times 16}$, we have obtained by computer the detailed expressions and the enumeration of all $15,296,512 \times 16 = 244,744,192$ orthomorphic permutation polynomials over $GF(16)$. We have verified that if $f(y) = a_0 + a_1 y + a_2 y^2 + \cdots + a_{15} y^{15}$ is an orthomorphic permutation polynomial over $GF(16)$, then $a_{14} = a_{15} = 0$.

We have also found that the number of orthomorphic permutation polynomials of order 1 over $GF(16)$ is 14×16, and the number of orthomorphic permutation polynomials of order 4, where $a_1 \neq 0, a_2 \neq 0, a_3 = 0, a_4 \neq 0$, is 300×16.

Combining the above results, we have the following theorem.

Theorem 3. *Let $f(y) = a_0 + a_1 y + a_2 y^2 + a_3 y^3 + \cdots + a_{q-1} y^{q-1}$ be an orthomorphic permutation polyno-*

mial over $F_2^m = \{0, 1, u, u^2, \cdots u^{q-2}\}$*, where* $q = 2^m, m = 2, 3, 4$*. Then* $a_{q-2} = 0$*, namely,* $deg(f(y)) \leq q - 3$*.*

We end this note by the following straightforward conjecture.

Conjecture 1. *Let* $f(y) = a_0 + a_1 y + a_2 y^2 + a_3 y^3 + \cdots + a_{q-1} y^{q-1}$ *be an orthomorphic permutation polynomial over* $F_2^m = \{0, 1, u, u^2, \cdots u^{q-2}\}$*, where* $q = 2^m, m \geq 2$ *is an integer. Then* $a_{q-2} = 0$*, namely,* $deg(f(y)) \leq q-3$*.*

From Identity (2), Conjecture 1 is equivalent to the following,

If $\{p[0], p[1], p[u], p[u^2], \cdots, p[u^{q-2}]\}$ is an orthomorphic permutation over $\{0, 1, u, u^2, \cdots u^{q-2}\}$ and $p[0] = 0$, then $p[1] + up[u] + u^2 p[u^2] + \cdots + u^{q-2} p[u^{q-2}] = 0$.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (No. 60473142).

References

[1] Z. Li, and X. Li, "Characterization and the counting method for orthomoriphic permutations," *Journal of Xidian University*, vol. 27, no. 6, pp. 809-812, 2000.

[2] Z. Li, R. Li, and X. Li, "Enumeration of orthomoriphic permutation polynomials over finite field F_8," *Journal of Shanxi Normal University*, vol. 29, no. 4, pp. 13-16, 2001.

[3] R. Lidl, and H. Niederreiter, *Finite Fields*, Addison-Wesley, 1983.

[4] Z. H. Liu, and C. Shu, "A method for constructing orthomorphic permutations of degree 2^m," *Chinacrypt '96*, pp. 56-59, Beijing: Science Press, 1996.

[5] L. Mittenthal, "Block substitutions using orthomorphic mappings," *Advances in Applied Mathematics*, vol. 16, no. 1, pp. 59-71, 1995.

Jianqin Zhou received his B.Sc. degree in mathematics from East China Normal University, China, in 1983, and M.Sc. degree in probability and statistics from Fudan University, China, in 1989. From 1989 to 1999 he was with the Department of Mathematics and Computer Science, Qufu Normal University, China. From 2000 to 2002, he worked for a number of IT companies in Japan. From 2003 to 2007 he was with the Department of Computer Science, Anhui University of Technology, China. From Sep 2006 to Feb 2007, he was a visiting scholar with the Department of Information and Computer Science, Keio University, Japan. Since 2008 he has been with the Telecommunication School, Hangzhou Dianzi University, China. He published more than fifty papers, and proved a conjecture posed by famous mathematician Paul Erdős et al. His research interests include coding theory, cryptography and combinatorics.