Non-linearity of Exponent Permutations*

Josef P. Pieprzyk
Department of Computer Science
University College
University of New South Wales
ADFA
Canberra, ACT 2600, AUSTRALIA

Abstract

The paper deals with an examination of exponent permutations with respect to their non-linearity. The first part gives the necessary background to be able to determine permutation non-linearity. The second examines the interrelation between non-linearity and Walsh transform. The next part summarizes results gathered while experimenting with different binary fields. In the last part of the work, we discuss the results obtained and questions which are still open.

*Support for this research was provided in part by the Australian Research Council under reference number A48830241

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 80-92, 1990.

1 Introduction

In [PF88] the authors analysed the non-linearity of permutations as one of the indicators of their quality for cryptographic use. They have given the upper boundary on non-linearities. Of course an application of permutations of the maximum non-linearity does not guarantee that an encryption algorithm based on them generates a "strong" cipher. For example the well-known DES algorithm is built using 32 permutations (each S-box consists of four permutations) and none of them attains the maximum non-linearity. Of course the selection of permutations in the DES has been made using a collection of properties (some of which may still remain unidentified). For the most complete list of such properties see [Bro88].

It has been shown in [PF88] that there are permutations whose non-linearity attains the upper bound for Galois fields $GF(2^3)$, $GF(2^4)$, and $GF(2^5)$. Unfortunately, it is not known if such permutations exist for larger binary fields (for $n > 5$). Experiments we have done point out that such permutations exist and can be easily obtained using exponentiation.

2 Background

Consider a Boolean function $f \in \mathcal{F}_n$ where $\mathcal{F}_n$ is the set of all Boolean functions of n variables. Its non-linearity N_f is defined as the Hamming distance between the function f and the set of all linear functions $\mathcal{L}_n$ existing in $\mathcal{F}_n$ i.e.

$$N_f = d(f, \mathcal{L}_n) = \min_{\alpha \in \mathcal{L}_n} d(f, \alpha) \tag{1}$$

For a given permutation $\mathrm{f} \in \mathcal{P}_n$, where $\mathcal{P}_n$ is the set of all permutations over $GF(2^n)$, we define its non-linearity as

$$\mathcal{N}_{\mathrm{f}} = \min_i (N_{f_i}, N_{f_i^{-1}}) \tag{2}$$

where $\mathrm{f} = (f_1, f_2, ..., f_n)$ and $\mathrm{f}^{-1} = (f_1^{-1}, f_2^{-1}, ..., f_n^{-1})$ are coordinates of the original and the inverse permutation, respectively.

In [PF88], it has been shown that there is a bound on non-linearity which can be attained by permutations for a given dimension n. The dimension n also can be seen as the number of binary inputs of a permutation block. The bound $\mathcal{N}_n$ is expressable by the following formula

$$\mathcal{N}_n = \begin{cases} \sum_{i=1/2(n-3)}^{n-3} 2^{i+1} & \text{if } n = 3, 5, 7, ... \\ \sum_{i=1/2(n-4)}^{n-4} 2^{i+2} & \text{if } n = 4, 6, 8, ... \end{cases} \tag{3}$$

We note that all permutations in $\mathcal{P}_2$ are linear so their non-linearities are equal to zero.

When designing cryptographic algorithms, one looks for those permutations which are both easy to implement and demonstrate a satisfactorily high non-linearity. Although the definition given in (2) is good to characterize non-linearity, we can also determine non-linearity of a permutation $\mathrm{f} \in \mathcal{P}_n$ as follows:

$$\mathcal{N}_{\mathrm{f}} = \frac{\sum_{i=1}^{n} N_{f_i} + \sum_{i=1}^{n} N_{f_i^{-1}}}{2n} \tag{4}$$

For example (see [PF88]) all permutations applied in the DES have the same non-linearity measured by the formula (2) and equal to 2 which is a half of the possible maximum. If we take the definition (4), then they have different non-linearities which vary from 3.73 (there are 6 of them; one in S_1 and S_8 and two in S_2 and S_6) to 3.00 (there are 4 of them; single permutations in S_2, S_6, S_7, and S_8). The average non-linearity of permutations in the DES is equal to 3.408 and is close to the maximum that is 4. For details see [PF88].

In fact in DES, all the permutations are used in their original form (their inverses are never applied during either enciphering and deciphering process). So if we count non-linearities of coordinates of the original permutations only, we find only 14 out of 32 that reach the maximum non-linearity.

The non-linearity of permutations given in (2) can be calculated differently as we can apply the following theorem.

Theorem 2.1 *Given a permutation* f, *its non-linearity can be calculated as*

$$\begin{aligned} N_f &= \min_{\alpha \in \mathcal{L}_n^n} \min_{i=1,\ldots,n} N_{(\mathrm{f} \star \alpha)_i} \\ &= \min_{\alpha \in \mathcal{L}_n^n} \min_{i=1,\ldots,n} N_{(\mathrm{f}^{-1} \star \alpha)_i} \end{aligned} \tag{5}$$

where $\mathcal{L}_n^n$ *is a set of all linear permutations, and* $(\mathrm{f} \star \alpha)_i$ *stands for i-th coordinate of the composite permutation* $\mathrm{f} \star \alpha$.

Proof: Clearly the set of all coordinates of all linear permutations creates the set $\mathcal{L}_n - \{0, 1\}$. For our permutation f, we can define the following set

$$\mathcal{L}_{\mathrm{f}} = \{g \in \mathcal{F}_n; g = a_0 \oplus a_1 f_1 \oplus \ldots \oplus a_n f_n\} \tag{6}$$

where a_i are binary elements and the set

$$\mathcal{L}_{\mathrm{f}^{-1}} = \{g \in \mathcal{F}_n; g = a_0 \oplus a_1 f_1^{-1} \oplus \ldots \oplus a_n f_n^{-1}\} \tag{7}$$

The both sets consist of all Boolean functions which are coordinates of compositions $\mathrm{f} \star \alpha$ and $\mathrm{f}^{-1} \star \alpha$, respectively. Notice that as α is a linear permutation, non-linearities of f and $\mathrm{f} \star \alpha$ coordinates are the same.

Observe that the relation between two sets $(\mathcal{L}_n , \mathcal{L}_{\mathrm{f}})$ and $(\mathcal{L}_n , \mathcal{L}_{\mathrm{f}^{-1}})$ is symmetric. This is to say that if we create a composition of $\mathrm{f} \star \mathrm{f}^{-1}$ the set $\mathcal{L}_{\mathrm{f}}$ plays the same role to the inverse as the set $\mathcal{L}_n$ to the original. If we take the second possibility $\mathrm{f}^{-1} \star \mathrm{f}$, we can draw the same conclusion for sets $\mathcal{L}_{\mathrm{f}^{-1}}$ and $\mathcal{L}_n$. In other words, the non-linearity of a permutation can be expressed as a distance between two sets $\mathcal{L}_n$ and $\mathcal{L}_{\mathrm{f}}$ or equivalently between $\mathcal{L}_{\mathrm{f}^{-1}}$ and $\mathcal{L}_n$.

□

We can conclude from the theorem that if there is at least one permutation coordinate that may be expressed by linear combination of the rest of the coordinates, this permutation has "0" non-linearity. It means that the inverse has at least one linear coordinate.

It has been shown [PF88] that it is easy to generate permutations of the maximum non-linearity at random for $GF(2^3)$ and $GF(2^4)$. Unfortunately, the generation of such permutations becomes more and more difficult as the dimension of Galois field grows.

Ideally, we would like to have a method that would generate permutations of the maximum non-linearity or at least close enough to it. We are going to examine an exponential function and its application to the generation of non-linear permutations for different dimensions n of a Galois field.

3 Walsh transform and non-linearity

Spectral tests are useful tools for detecting non-randomness in binary strings. Originally the first such test was proposed by Gait [Gai77] who used the discrete Fourier transform to examine binary strings generated by the DES. At the same time Yuen [Yue77] suggested another test based on the Walsh transform which was later improved by Feldman [Fel87]. As Forre [For88] has shown the Walsh transform can also be used to estimate the strict avalanche criterion of Boolean functions.

Before we show the relation between the Walsh transform and non-linearities of Boolean functions, we give the necessary definitions and notions. Assume we have a Boolean function $f \in \mathcal{F}_n$ of n variables $\vec{x}$=$(x_1,...,x_n)$. As the Walsh transform may be applied to real-valued functions only, we treat $f(\vec{x})$ as such a function. It is taken as 0 if it is false and 1 if it is true. The Walsh transform $F(\vec{\omega})$ of $f(\vec{x})$ is defined as (see [Bea75]):

$$F(\vec{\omega}) = \sum_{\vec{x}\in Z_2^n} f(\vec{x})(-1)^{\vec{\omega}\cdot\vec{x}} \tag{8}$$

where Z_2^n is a space of all binary sequences of length n, $f(\vec{x})$ is the transformed function (considered as a real-valued function), and $\vec{\omega} \cdot \vec{x}$ stands for the dot-product of $\vec{\omega}$ and $\vec{x}$:

$$\vec{\omega} \cdot \vec{x} = \omega_1 x_1 \oplus \omega_2 x_2 \oplus \cdots \oplus \omega_n x_n. \tag{9}$$

Having $F(\vec{\omega})$, we can recreate the function $f(\vec{x})$ using the inverse Walsh transform that is:

$$f(\vec{x}) = 2^{-n} \sum_{\vec{\omega}\in Z_2^n} F(\vec{\omega})(-1)^{\vec{\omega}\cdot\vec{x}}. \tag{10}$$

First notice that the Walsh spectrum of a linear Boolean function has a specific form which is described by the following theorem.

Theorem 3.1 *The Walsh transform $F(\vec{\omega})$ of a linear Boolean function has two non-zero components only.*

Proof: Clearly, the first non-zero component is

$$F(0) = \sum_{\vec{x}\in Z_2^n} f(\vec{x}) \tag{11}$$

as $\vec{\omega} \cdot \vec{x}$=0 for $\vec{\omega}$=0 and therefore $(-1)^{\vec{\omega}\cdot\vec{x}}$=1. In other words $F(0)$ gives the number of 1's (the number of TRUE values) in the function f.

Notice that for a fixed $\vec{\omega}$, its dot product $\vec{\omega} \cdot \vec{x}$ indicates the linear function

$$l_\omega(\vec{x}) = \omega_1 x_1 \oplus ... \oplus \omega_n x_n.$$

Clearly, $\vec{\omega}$ generates a half of all linear functions of n Boolean variables (recall that we assign value "0" to the FALSE and value "1" to the TRUE). The rest may be obtained using negation

$$\overline{l_\omega(\vec{x})} = \omega_1 x_1 \oplus ... \oplus \omega_n x_n \oplus 1.$$

So if we have a linear function f, it is either of the form

$$\omega'_1 x_1 \oplus ... \oplus \omega'_n x_n$$

or

$$\omega'_1 x_1 \oplus ... \oplus \omega'_n x_n \oplus 1$$

for a suitable sequence of $\vec{\omega}' = (\omega'_1, ..., \omega'_n)$. There are three possible cases:

- f is different from a linear function generated by the dot product given by $\vec{\omega}$". In that case the Hamming distance between f and the linear function $l_{\omega^n}(\vec{x})$ is equal to $2^n - 1$. It means that
$$F(\vec{\omega}") = \sum_{\vec{x} \in Z_2^n} f(\vec{x})(-1)^{\vec{\omega}".\vec{x}} = 0;$$
- f is equal to a linear function $l_{\omega^n}(\vec{x})$ generated by the dot product then the Hamming distance between these two is equal to 0. It implies that f=1 while $\vec{\omega}" \cdot \vec{x} = 1$ so $F(\vec{\omega}")$=-2^{n-1} ;
- f is a complement of $l_{\omega^n}(\vec{x})$ generated by the dot product, then $d(f,l)$=2^n and f=1 while $l_{\omega^n}(\vec{x})$=0 so $F(\vec{\omega}")$=$+2^{n-1}$;

One of the last two gives the second non-zero component of the Walsh spectrum.

□

The next theorem explains the interrelation between non-linearity of a Boolean function and its Walsh spectrum.

Theorem 3.2 *If a given Boolean function $f(x_1, ..., x_n)$ has its non-linearity equal to η, then*

$$\eta = \min(\min_{\vec{\omega} \neq 0}(2^{n-1} - \mid F(\vec{\omega}) \mid), 2^n - \mid F(0) \mid, \mid F(0) \mid). \tag{12}$$

Proof: As we know the dot product generates a half of all linear functions. If the non-linearity of f is equal to η, then there is a linear function α such that

$$\eta = d(f, \alpha). \tag{13}$$

Therefore we consider two cases.

- Case I - the closest linear function α can be expressed by an element of the dot-product set, that is
$$\alpha(\vec{x}) = \vec{\omega}' \cdot \vec{x}. \tag{14}$$
So
$$\begin{aligned} F(\vec{\omega}') &= \sum_{\vec{x} \in Z_2^n} f(\vec{x})(-1)^{\vec{\omega}' \cdot \vec{x}} \\ &= \sum_{\vec{x} \in Z_2^n} \alpha(\vec{x})(-1)^{\vec{\omega}' \cdot \vec{x}} \\ &- \sum_{\vec{x}; f(\vec{x}) \neq \alpha(\vec{x}); \vec{\omega}' \cdot \vec{x} = 1} (-1)^1 + \sum_{\vec{x}; f(\vec{x}) \neq \alpha(\vec{x}); \vec{\omega}' \cdot \vec{x} = 0} (-1)^0. \end{aligned} \tag{15}$$
As the first part of the formula
$$\sum_{\vec{x} \in Z_2^n} \alpha(\vec{x})(-1)^{\vec{\omega}' \cdot \vec{x}} = -2^{n-1} \tag{16}$$
and the rest is equal to η, we get
$$F(\vec{\omega}') = -2^{n-1} + \eta. \tag{17}$$

- case II - the closest linear function can be expressed by a negation of an element of the dot-product set. It means that
$$\eta = d(f, \overline{\alpha}), \tag{18}$$
and
$$\begin{aligned} F(\vec{\omega}') &= \sum_{\vec{x} \in Z_2^n} f(\vec{x})(-1)^{\vec{\omega}' \cdot \vec{x}} \\ &= \sum_{\vec{x} \in Z_2^n} \overline{\alpha(\vec{x})}(-1)^{\vec{\omega}' \cdot \vec{x}} \\ &+ \sum_{\vec{x}; f(\vec{x}) \neq \overline{\alpha(\vec{x})}; \vec{\omega}' \cdot \vec{x} = 1} (-1)^1 - \sum_{\vec{x}; f(\vec{x}) \neq \overline{\alpha(\vec{x})}; \vec{\omega}' \cdot \vec{x} = 0} (-1)^0. \end{aligned} \tag{19}$$
The first part of the formula is given by
$$\sum_{\vec{x} \in Z_2^n} \overline{\alpha(\vec{x})}(-1)^{\vec{\omega}' \cdot \vec{x}} = 2^{n-1} \tag{20}$$
and the rest is equal to η. So, we get
$$F(\vec{\omega}') = 2^{n-1} - \eta. \tag{21}$$

Considering both cases, we can write that
$$\eta = 2^{n-1} - \mid F(\vec{\omega}') \mid . \tag{22}$$

Finally, if we consider the case for $\vec{\omega}=0$, we obtain the result.

□

Theorem 3.1 says that any linear Boolean function is easily identified by looking at its Walsh spectrum. In general any linear permutation over $GF(2^n)$ has a specific Walsh spectrum. Before we present the relation between linear permutations and their Walsh spectra, let us consider the following theorem which expresses the dependence between Walsh spectra of permutations and their coordinates.

Theorem 3.3 *Given a permutation* f $\in \mathcal{P}_n$. *If $F_i(\vec{\omega})$ is the Walsh transform of i-th coordinate of the permutation (i=1,...,n), then the Walsh transform of* f *is expressable as*
$$F(\vec{\omega}) = \sum_{i=1}^{n} 2^{i-1} F_i(\omega) \tag{23}$$
where f $= (f_1, ..., f_n)$ *and* $F_i \leftrightarrow f_i$.

Proof: For any value of $\vec{x}$, f$(\vec{x}) = f_1 + 2f_2(\vec{x}) + ... + 2^{n-1}f_n(\vec{x})$. Using the definition of the Walsh transform (8), we get the final result.

□

The above theorem gives us, the following conclusion.

Collorary 3.1 *If a permutation* $\mathrm{f} \in \mathcal{P}_n$ *is linear, then its Walsh transform has* $n-1$ *non-zero components. The first component is given by*

$$F(0) = 2^{n-1} \sum_{i=1}^{n} 2^{i-1} \tag{24}$$

and the other n *components create a permutation of* n *integers* $(\pm 2^{n-1}, \pm 2^{n}, ..., \pm 2^{2(n-1)})$

Example. Consider the identity permutation over $GF(2^3)$. The permutation $\mathrm{f} = (f_1, f_2, f_3)$ is shown in the table below. Its Walsh spectrum is given in the same table where F_1, F_2, F_3 are Walsh spectra of the Boolean functions f_1, f_2, f_3, respectively, and F is the spectrum of the permutation.

$\vec{x}/\vec{\omega}$	f_1	f_2	f_3	f	F_1	F_2	F_3	F
000 (0)	0	0	0	0	4	4	4	28
001 (1)	0	0	1	1	-4	0	0	-4
010 (2)	0	1	0	2	0	-4	0	-8
011 (3)	0	1	1	3	0	0	0	0
100 (4)	1	0	0	4	0	0	-4	-16
101 (5)	1	0	1	5	0	0	0	0
110 (6)	1	1	0	6	0	0	0	0
111 (7)	1	1	1	7	0	0	0	0

4 Exponent permutations

In [PF88] it has been shown that there are permutations of the maximum non-linearity for n=3,4,5 and 6. For $n \geq 7$, it is very hard to find such permutations. It would be interesting if we could find such permutations using a simple method. Experiments have shown exponentiation generates permutations whose non-linearities tend to be close to the maximum.

In general, we have dealt with permutations of the form:

$$\mathrm{f}(x) = (h(x))^k mod\, g(x) \tag{25}$$

where $g(x)$ is an irreducible polynomial of degree n which generates a Galois field $GF(2^n)$ and $h(x)$ represents elements of $GF(2^n)$.

Example. Consider $GF(2^3)$ generated by $g(x){=}x^3 + x^2 + 1$ and two permutations: the first

$$\mathrm{f}_1(x) = (h(x))^2 (mod\, g(x)) \tag{26}$$

and the second

$$\mathrm{f}_2(x) = (h(x))^3 (mod\, g(x)) \tag{27}$$

The permutations along with their Walsh transforms are presented in the tables below:

$\bar{x}/\bar{\omega}$	f	F_1	F_2	F_3	F
0	0	4	4	4	28
1	1	-4	0	0	-4
2	4	0	0	0	0
3	5	0	0	0	0
4	7	0	-4	0	-8
5	6	0	0	0	0
6	3	0	0	-4	-16
7	2	0	0	0	0

and

$\bar{x}/\bar{\omega}$	f	F_1	F_2	F_3	F
0	0	4	4	4	28
1	1	2	0	0	2
2	5	0	-2	0	-4
3	2	-2	-2	0	-6
4	6	0	-2	-2	-12
5	4	-2	2	-2	-6
6	7	0	0	-2	-8
7	3	-2	0	2	6

The first permutation is linear. The second, however, attains the maximum non-linearity for all its coordinates. The Walsh transforms F of the whole permutation can be easily computed from Walsh transforms of its coordinates (F_1,F_2,F_3) according to $F(\bar{\omega})=F_1 + 2F_2 + 4F_3$.

The first permutation in the example illustrates the general property of exponent permutation that can be expressed as

Collorary 4.1 *Any permutation*

$$(h(x))^k \bmod g(x) \tag{28}$$

where $g(x)$ is a generator of $GF(2^n)$, is a linear permutation for k=1,2,4,...,2^{n-1}

The collorary results from the well-known fact that squaring in any binary field $GF(2^n)$ is a linear operation - for details see [Ber68].

The second permutation has a very regular pattern of integers in its Walsh transforms. It is no coincidence. In other words (see [PF88]), the space of all linear functions $\mathcal{L}_n$ may be divided into two sets with respect to any coordinate. The first subset consists of all linear functions whose Hamming distances to the given coordinate are equal 2^{n-1} (corresponding Walsh transforms are equal 0). The second subset comprises all linear functions whose distances to the given coordinate are either $2^{n-1} - 2^{(n-1)/2}$ or $2^{n-1} + 2^{(n-1)/2}$. It means that the corresponding Walsh components are equal $\pm 2^{(n-1)/2}$ and therefore their non-linearities are equal to $2^{(n-1)} - 2^{(n-1)/2}$. This observation is valid for n odd and greater than 1.

Concatenation of exponential blocks gives the identity permutation if and only if the product of all exponents is equal to 1 modulo $(2^n - 1)$. Consider squaring. Exponents after using subsequent squaring are as follows:

$$2^2,\ 2^3,\ \dots\ 2^n \tag{29}$$

Note that the last element $2^n = 1\,mod\,(2^n - 1)$ and it corresponds to concatenation of n blocks. In general, if we deal with an exponential permutation described by an exponent 2^i where $i = 2, 3, \dots, n-1$, then we may construct the following sequence of exponents:

$$2^i,\ 2^{2i},\ \dots, 2^{ni} = 1\ (mod\,2^n - 1) \tag{30}$$

This leads us to the next conclusion (see [Ber68]).

Collorary 4.2 *If n is prime, then all linear exponents* $(2, 4, 8, 16, \dots)$ *have the same minimal length of concatenation n after which we have got the identity permutation.*

Collorary 4.3 *If n is not prime, then for any linear permutation described by its exponent 2^i, we can find such an integer k $(k < n)$ that $2^{ki} = 2^n$, where k and i are factors of n. It means that we can use a smaller number of exponential blocks to create the identity permutation.*

Consider an exponent permutation $f(\alpha) = \alpha^a$ in $GF(2^n)$ given by its exponent a. Any concatenation of the same $\phi(2^n - 1)$ exponential blocks (permutations) gives the identity permutation, where $\phi(N)$ is the Euler ϕ-function or the Euler totient function - see [Ber68]. So all exponents can be divided into several disjoined classes depending upon their orders modulo $2^n - 1$ that have to be factors of $\phi(2^n - 1)$.

If $2^n - 1$ is a prime, then $\phi(2^n - 1) = 2^n - 2$ and there is always an exponent e that generates, by exponentiation, all other nonzero exponents. It is called a primitive element of the cyclic group CG created by all nonzero elements of $GF(2^n)$ and with multiplication as the group operation. In other words the sequence of exponents

$$e,\ e^2,\ e^3,\ \dots\ e^{2^n - 2} \tag{31}$$

generates all possible exponential permutations. Thus we have got the following conclusion.

Collorary 4.4 *If $2^n - 1$ is a prime, then concatenation of $\frac{2^n - 2}{n}$ exponential blocks defined by a primitive element e of CG generates a linear permutation.*

Take an exponent e of order m modulo $2^n - 1$ (e has order m modulo $2^n - 1$ if $e^m = 1\,mod 2^n - 1$) and m is different from 2, then we can create concatenation of two blocks: the first expressed by e, and the second by 2^i; $i = 1, \dots, n-1$ and its order is $n \cdot m$ but its non-linearity stays the same.

We have experimented extensively, starting the search with n=3. The set of all exponent permutations is modest and it splits into two subsets. Elements of {1,2,4} give linear permutations. The set {3,5,6} consists of all non-linear permutations and corresponding permutations share the same, maximum non-linearity which is equal to 2. In fact, we use the only independent non-linear exponent $e = 3$. Exponent 5 is the inverse of 3 so $5 = 3^{-1}$, but $6 = 6^{-1} = 2 \cdot 3$. Therefore all three exponent must have the same non-linearity.

In space $GF(2^4)$, we can identify the set of linear exponents {1,2,4,8} and the set of non-linear ones {7,11,13,14}. The rest of exponents do not give permutations - they are factors of

$2^4-1=15$ and they do not have their inverses. Non-linear exponent permutations have the same maximum non-linearity equal to 4.

For $n=5$, 2^5-1 is a prime and $\phi(31)=30$, so there are four basic subsets of exponents (elements of CG). Each basic set contains elements of the same order modulo 2^n-1. The basic sets are as follows:

$$\begin{aligned} Z_1 &= \{1\} \\ Z_2 &= \{30\} \\ Z_3 &= \{5,25\} \\ Z_5 &= \{2,4,8,16\} \end{aligned}$$

and they correspond to the factorization of the integer $\phi(31)$. Sets Z_5 and Z_1 contain all linear exponents. Z_2 has the only element which gives a permutation of non-linearity 10. The set Z_3 consists of two permutations of the maximum non-linearity (equal to 12). The rest of exponents (permutations) can be seen as a product of exponents from the basic sets Z_2, Z_3, and Z_5. If we create them using Z_2 and Z_3, we have $Z_6=Z_2 \times Z_3=\{14,26\}$ - both elements have non-linearity 12, where $Z_2 \times Z_3$ means the set whose elements are of the form $e = e' \times e"$; $e' \in Z_2$, $e" \in Z_3$. Finally, we obtain

$$\begin{aligned} Z_{10} = Z_2 \times Z_5 &= \{15,23,27,29\} \\ Z_{15} = Z_3 \times Z_5 &= \{7,9,10,14,18,19,20,28\} \\ Z_{30} = Z_2 \times Z_3 \times Z_5 &= \{3,11,12,13,17,21,22,24\} \end{aligned}$$

Non-linearities are 10,12,12 for Z_{10}, Z_{15}, Z_{30}, respectively.

The case of $n=6$ is especially interesting. As $2^6-1=63$ and $\phi(63)=36=6\cdot 6$, all orders of exponents must be factors of 6. Therefore we get

$$\begin{aligned} Z_1 &= \{1\} \\ Z_2 &= \{8,55,62\} \\ Z_3 &= \{4,16,22,25,37,43,46,58\} \\ Z_6 &= \{2,5,10,11,13,17,19,20,23,26,29,31, \\ &\quad 32,34,38,40,41,44,47,50,52,53,59,61\} \end{aligned}$$

The set Z_2 consists of one linear exponent and two of the maximum non-linearity (equal to 24). All non-linear elements of Z_3 share the same non-linearity 20. The set Z_6 has a mixture of exponents of different non-linearities (0, 20, 24).

Consider $GF(2^7)$. In this field $2^7-1=127$ is prime and $\phi(127)=126=2\cdot 3^2\cdot 7$. The set of all exponents splits up into following subsets:

$$\begin{aligned} Z_1 &= \{1\} - non-linearity\ 0 \\ Z_2 &= \{126\} - non-linearity\ 54 \\ Z_3 &= \{19,107\} - non-linearity\ 44 \\ Z_7 &= \{2,4,8,16,32,64\} - non-linearity\ 0 \\ Z_9 &= \{22,37,52,68,99,103\} - non-linearities\ 44\ and\ 56 \\ Z_6 &= Z_2 \times Z_3 - non-linearity\ 56 \end{aligned}$$

$$\begin{aligned}
Z_{14} &= Z_2 \times Z_7 - \mathit{non-linearity}\ 54 \\
Z_{18} &= Z_2 \times Z_9 - \mathit{non-linearities}\ 44\, \mathit{and}\, 56 \\
Z_{21} &= Z_3 \times Z_7 - \mathit{non-linearity}\ 44 \\
Z_{42} &= Z_6 \times Z_7 - \mathit{non-linearity}\ 56 \\
Z_{63} &= Z_9 \times Z_7 - \mathit{non-linearities}\ 44\, \mathit{and}\, 56 \\
Z_{126} &= Z_2 \times Z_{63} - \mathit{non-linearities}\ 44\, \mathit{and}\, 56
\end{aligned}$$

For example exponents 3 and 7 belong to Z_{126} (they are primitive elements of CG) but their non-linearities are different. The exponent e=3 yields the permutation of the maximum non-linearity (which is 56) while e=7 produces the permutation of non-linearity 44.

Our experiments, let us draw the following conclusions:

- non-linearity of exponent permutations does not depend on the primitive polynomial that generates $GF(2^n)$,
- non-linearity of exponent permutations does depend upon the internal structure of CG,
- non-linearity of the permutation for a given exponent that is a primitive element of CG does not necessarily attain the maximum,
- concatenation of $\frac{\phi(2^n-1)}{n}$ the same exponent permutations generates a linear permutation.

5 Conclusions

Boolean functions can be characterized by their non-linearities. We have assumed a definition of non-linearity as the minimum distance between a given function and the set of all linear Boolean functions. Non-linearity of a function can be determined by looking at its Walsh transform. In general, the Walsh transform of a Boolean function can be seen as a projection of the function into the vector basis created by linear functions. Functions of the maximum non-linearity have a specific pattern of their Walsh spectra. It means that they are pretty rare in the space of all Boolean functions of a given dimension n. The probability of choosing such a function at random diminishes as the space dimension grows.

Walsh transforms can be applied to generate Boolean permutations of the maximum non-linearity. Clearly, a permutation is a collection of n Boolean functions (coordinates). Any such a function has its Walsh spectrum which consists of $2^{n-1}-1$ zeros, 2^{n-1} elements are equal $\pm(2^{n-1}-\eta)$ where η is the maximum non-linearity, and the last element $F(0)$ is always equal to 2^{n-1}. Among themselves, Walsh spectra of coordinates have to fulfil the same conditions as Boolean functions do. So, for any pair of coordinates, a pair of suitable nonzero Walsh spectrum elements $F(\bar{\omega})$ ($\bar{\omega} \neq 0$) must overlap for 2^{n-2} elements (signs do not matter).

Exponentiation is an convenient way to produce permutations of the maximum or close to maximum non-linearity. The production of non-linear Boolean function or non-linear permutations in $GF(2^n)$ is required in many applications for example while designing cryptographic algorithms, pseudorandom generators, etc. Squaring is always a linear operation in $GF(2^n)$ but cubing provides a permutation of the maximum non-linearity for n=3,5,7,9, note that for n=4,6,8,... , it does not generate a permutation as 3 divides 2^n-1. It seems that any generator of a multiplicative group CG should share the same non-linearity as each generator produces by concatenation all possible exponent permutations. We have found that this statement is not true in general. There are, however, many still open questions about exponent permutations and their non-linearities. Some of them are listed below.

1. What is the relation between the value of an exponent and its permutation non-linearity ?
2. What is the dependence between the order modulo $2^n - 1$ of an exponent and its permutation non-linearity ?
3. What is the non-linearity spectrum of all exponents which produce permutations ?
4. What is the non-linearity spectrum of primitive generators of CG ?
5. Do permutations for $e = 3$ attain the maximum for all $GF(2^n)$, where n is odd ?
6. Does non-linearity of exponent permutations depend upon a field generator for larger n or not ?

There is a common consensus that non-linearity is a desirable cryptographic feature. However, in practice, while choosing non-linear permutations for a DES-like cryptographic algorithm, we face the question of whether permutations of the maximum non-linearity are "good" from a cryptographic point of view or permutations of the average non-linearity are better. Although exponent permutations are sucessfully being used in both the Rivest-Shamir-Adleman and the Diffie-Hellman cryptosystems and exponentiation itself is difficult to invert if you are dealing with large enough instance (large enough $GF(2^n)$), it is difficult to say if exponent permutations for small parameters n could generate a "strong" enciphering algorithm.

Considering the fact that concatenation of any $\frac{\phi(2^n-1)}{n}$ exponent permutations generates a linear one, we notice that a well known iteration attack (see [SN77] or [SP88]) on exponential cryptosystems is more efficient in $GF(2^n)$. The iteration attack has always worked well if there is a small number of concatenations of exponent permutations (the exponent permutation is given by a public key) that give the identity permutation. In $GF(2^n)$, however, it is sufficient to create a concatenation of exponent permutations which produces a linear permutation. As the set of all linear permutations is closed according to the inversion operation, we can easily find the inverse linear permutation and generate the identity permutation.

ACKNOWLEDGMENT

I would like to thank Professor Jennifer Seberry for her critical comments and presenting this paper on my behalf during EUROCRYPT'89. It is also a pleasure to thank Sophie Richards and Patrick Tang for their assistance during preparation of this work.

References

[Bea75] K. G. Beauchamp. *Walsh Functions and Their Applications.* Academic Press, New York, 1975.

[Ber68] E. R. Berlekamp. *Algebraic Coding Theory.* MacGraw-Hill Book Company, New York, 1968.

[Bro88] L. Brown. A proposed design for an extended DES. IFIP TC11, International Conference on Computer Security : IFIP/SEC'88, W.J. Caelli (ed), Elsevier (to appear), May 1988. Abstracts, Gold Coast, Queensland, Australia.

[Fel87] F. A. Feldman. Fast spectral tests for measuring nonrandomness and the DES. Papers and Abstracts, CRYPTO'87, 1987.

[For88] R. Forre. The strict avalanche criterion: spectral properties of Boolean functions and an extended definition. Papers and Abstracts, CRYPTO'88, August 1988.

[Gai77] J. Gait. A new nonlinear pseudorandom number generator. *IEEE Transactions on Software Engineering*, SE-3(5):359–363, September 1977.

[PF88] J. P. Pieprzyk and G. Finkelstein. Towards an effective non-linear cryptosystem design. IFIP TC11, International Conference on Computer Security : IFIP/SEC'88, W.J. Caelli (ed), Elsevier (to appear), May 1988. Abstracts, Gold Coast, Queensland, Australia.

[SN77] G. J. Simmons and M. J. Norris. Preliminary comments on the MIT public-key cryptosystem. *Cryptologia*, Vol.1:406–414, 1977.

[SP88] J. Seberry and J. Pieprzyk. *Cryptography: An Introduction to Computer Security.* Prentice Hall, Inc., Englewood Cliffs, New Jersey, 1988.

[Yue77] C. Yuen. Testing random number generators by Walsh transform. *IEEE Transactions on Computers*, C-26(4):329–333, April 1977.