On Almost Perfect Nonlinear Permutations

T. Beth and C. Ding

European Institute for System Security
University of Karlsruhe
P.O. Box 6980, Am Fasanengarten 5
D-W7500 Karlsruhe 1, Germany

abstract. In this paper basic properties of APN permutations, which can be used in an iterated secret-key block cipher as a round function to protect it from a differential cryptanalysis, are investigated. Several classes of almost perfect nonlinear permutations and other permutations in $GF(2)^n$ with good nonlinearity and high nonlinear order are presented. Included here are also three methods for constructing permutations with good nonlinearity.

1 Introduction

Many secret-key block ciphers are based on iterating a substitution function several times. Each iteration is called a round. Such a substitution function is refered to as the round function. The Security of such iterated block ciphers depends mainly on the "strength" of the round function. It is known that the nonlinearity of the round function is crutial for the security of an iterated block cipher.

There are two related concepts for nonlinearity of a substitution function: local nonlinearity and global nonlinearity. Let $f(x)$ be a substitution function of $GF(q)$, then

$$P_f(\alpha) = \max_{\gamma} P(f(X+\alpha) - f(X) = \gamma), \alpha \neq 0$$

is the measure of the local nonlinearity and

$$P_f = \max_{\alpha \neq 0} P_f(\alpha)$$

is that of the global nonlinearity of $f(X)$.

The linearity and nonlinearity of some cipher functions have been analyzed by Chaum and Evertse [3], Biham and Shamir [1, 2], Lai, Massey and Murphy [4], Nyberg and knudsen [5], Pieprzyk [6]. The differential cryptanalysis of DES-like functions introduced by Biham and Shamir [1,2] are closely related with the nonlinearity of cryptofunctions. As shown by Biham and Shamir [1,2], Lai, Massey and Murphy [4], Nyberg and Knudsen [5], to make an iterated block cipher immune to a differential cryptanalysis, it suffices to make the global nonlinearity P_f of the round function as small as enough.

T. Helleseth (Ed.): Advances in Cryptology - EUROCRYPT '93, LNCS 765, pp. 65-76, 1994.

For a round function f over $GF(2)^n$, the minimum value for P_f is 2^{1-n}. Permutations of $GF(2)^n$ with $P_f = 2^{1-n}$ were said to be almost perfect nonlinear(APN)[5]. In [5] Nyberg and Knudsen have given some results about quardatic APN permutations. In this paper basic properties of APN permutations in $GF(2)^n$ are developed in Section 2. Section 3 presents results about the relationships between permutations in $GF(2^n)$ and in $GF(2)^n$. Section 4 gives quadratic permutations with controllable nonlinearity. Section 5 provides with a class of permutations of order 3 with good nonlinearity. Section 6 presents a class of APN permutations in $GF(2)^n$ with maximum order $n-1$. Section 7 gives a class of permutations of order $n-2$ with controllable nonlinearity. Section 8 discusses the nonlinearity of the permutations X^d in $GF(2^n)$ with $d = 2^m - 1$.

2 Properties of APN Permutations

First of all, we would like to mention that the concept of nonlinearity is associated with a definite operation. In this paper we only discuss the nonlinearity of permutations in $GF(2^n)$ and in $GF(2)^n$ under the additions of them respectively.

From the definition of APN permutation, it is apparent that the following Lemma 1 holds:

Lemma 1 *Let $f(x)$ be a permutation of $GF(2)^n$ and $g(x,a) = f(x) + f(x+a)$. Then $f(x)$ is APN iff $g(x,a)$ takes exactly 2^{n-1} different nonzero vectors of $GF(2)^n$ and each of them two times when x runs over $GF(2)^n$ for each $a \neq 0$.*

It may be cryptographically beneficial to require that $g(x,a)$ takes each nonzero vector of $GF(2)^n$ equally likely, i.e. , $g(x,a)$ takes each vector of $GF(2)^n$ 2^n times when x runs over $GF(2)^n$ and a over $GF(2)^n - \{0\}$. We call such functions difference uniformly distributed (DUD). The $f(x)$ in the following Example 1 is APN, but not DUD. The permutation in Example 2 is APN and DUD.

Example 1 *Let $f(x) = (f_1, f_2, f_3)$ in $GF(2)^3$, where $f_1(x) = x_1 + x_2 + 1 + x_2x_3$, $f_2(x) = x_1 + x_3 + x_1(x_2 + x_3)$, $f_3(x) = x_2 + x_1x_3$.*

Example 2 *Let $f(x) = (f_1, f_2, f_3)$ in $GF(2)^3$, where $f_1(x) = x_1x_2 + x_1x_3 + x_1 + x_2$, $f_2(x) = x_1 + x_2x_3 + x_3$, $f_3(x) = 1 + x_1 + x_1x_2 + x_2x_3$.*

From Lemma 1 it follows that the following Theorem 1 holds:

Theorem 1 *Let $f(x) = (f_1(x), \cdots, f_n(x))$ be a permutation in $GF(2)^n$, then*
1) $f_i(x)$ is balanced, but not bent;
2) the order $ord(f_i) \leq n-1$;
3) if $f(x)$ is APN (DUD), then $h(x) = f(Ax+b)$ is also APN (DUD) for each nonsingular $n \times n$ matrix A over $GF(2)$ and each b in $GF(2)^n$.

Before to present a characterization of APN permutations, we need the following definitions and results:

Definition 1 *Let S be a subset of $GF(2)^n$-$\{0\}$. If for any $a \neq 0$, $b \neq 0$, $a+b \neq 0$, a, $b \in GF(2)^n$, there is at least one of the a, b, $a+b$, which belongs to S, then we call S a differential representation set of $GF(2)^n$. A differential representation set of $GF(2)^n$ such that $|S|$ is minimal, is called a differential basis of $GF(2)^n$, and $|S|$ is called the differential dimension (DD).*

Theorem 2 *A subset S of $GF(2)^n$ is a differential representation set of $GF(2)^n$ iff the difference of any two distinct elements of the set $GF(2)^n - S - \{0\}$ belongs to S.*

Theorem 3 *The differential dimension (DD) of $(GF(2)^n, +)$ is $2^{n-1}-1$ and the set $E = \{x : W_H(x)$ even, $x \in GF(2)^n, x \neq 0\}$ is a differential basis of $GF(2)^n$, where $W_H(x)$ denotes the Hamming weight of the vector x.*

Proof: Let S be any differential representation set of $GF(2)^n$, $|S| = k$, then $|S'| = |GF(2)^n - S - \{0\}| = 2^n - k - 1$. Suppose that $S' = \{s_1, \cdots, s_{2^n-k-1}\}$, then the elements s_1+s_2, s_1+s_3, $\cdots$, $s_1+s_{2^n-k-1}$, are distinct and all belongs to S, therefore we have $k \geq 2^n - k - 2$, which is equivalent to $k \geq 2^{n-1} - 1$. It is clear that E is a representation set of $GF(2)^n$ and $|E| = 2^{n-1} - 1$.

Theorem 4 *Let $D = \{d_1, \cdots, d_{2^{n-1}-1}\}$ be any differential basis of $GF(2)^n$, and $f(x)$ be a permutation in $GF(2)^n$. Then $f(x)$ is APN iff for each i, $g(x, d_i) = f(x)+f(x+d_i)$ takes exactly 2^{n-1} different nonzero vectors of $GF(2)^n$ and each two times.*

Proof: By definition the necessity is natural. What remains to be proved is the sufficiency. For any $a \neq 0$, $x \neq y$ and $x+y \neq a$, let $b = x+y$, then $b \neq a$, $b \neq 0$. Noticing that

$$\begin{aligned} d &= [f(x)+f(x+a)]+[f(y)+f(y+a)] \\ &= [f(x)+f(y)]+[F(x+a)+f(y+a)] \\ &= [f(x)+f(y+a)]+[f(x+a)+f(y)] \end{aligned}$$

and that there is at least one of the elements in $\{a,\ b,\ a+b\}$ that belongs to D, we have $d = 0$. This proves the sufficiency.

From Theorem 4 we see that $f(x)$ is APN iff for each nonzero vector e of even Hamming weight, $g(x, e)$ takes 2^{n-1} different nonzero vector of $GF(2)^n$. This result reduces largely the operation in searching for APN permutations.

Theorem 5 *Let $f(x) = (f_1(x), \cdots, f_n(x))$ be a APN permutation, then none of $f_1, \cdots, f_n$, is affine.*

Proof: Suppose that $f_1(x) = b_{1n}x_n + \cdots + b_{11}x_1 + b_0$, then

$$f_1(x) + f_1(x+c) = \sum_{i=1}^{n} b_{1i}c_i,$$

so we can find a vector $c \neq 0$ such that $f_1(x) + f_1(x+c) = 0$. whence

$$f(x) + f(x+c) = (0, f_2(x) + f_2(x+c), \cdots, f_n(x) + f_n(x+c)).$$

To ensure that $f(x)+f(x+c)$ takes 2^{n-1} distinct vectors of $GF(2)^n$, there must exist a vector x such that

$$f(x) + f(x+c) = (0, \cdots, 0).$$

This is contrary to the one-to-one property of $f(x)$. This completes the proof.

This theorem demonstrates that each component function of a APN permutation can not be affine. In what follows in this section, we shall discusss the nonlinear terms $x_i x_j (i \neq j)$ of APN permutations.

Theorem 6 *Let $f(x) = (f_1(x), \cdots, f_n(x))$ be a APN permutation of $GF(2)^n$. Then every quadratic term $x_i x_j (i \neq j)$ must appear in at least one of the component functions $f_1, \cdots, f_n$.*

Proof: For $c, x \in GF(2)^n$, let $x^c = 0$ when $x \neq c$, and $x^c = 1$ otherwise. Therefore $f(x)$ can be expressed as

$$\begin{aligned} f(x) &= \sum_{c \in GF(2)^n} x^c f(c) = \prod_{i=1}^{n} x_i \sum_{c \in GF(2)^n} f(c) \\ &\quad + \sum_{i=1}^{n-1} \sum_{1 \leq k_1 \leq \cdots \leq k_i \leq n} \Big(\prod_{j \neq k_1, \cdots, k_i} x_j \Big) \sum_{c} c'_{k_1} \cdots c'_{k_i} f(c) \end{aligned}$$

where $c'_i = 1 + c_i$. Without the loss of generality, we consider the cofficients of the term $x_{n-1}x_n$, which is

$$f(0 \cdots 001) + f(0 \cdots 000) + f(0 \cdots 010) + f(0 \cdots 011),$$

not equal to zero vector by the definition of APN permutations. This proves the theorem.

The nonlinear oder of a permutation $f(x) = (f_1(x), \cdots, f_n(x))$ is defined as

$$ord(f) = \max_{1 \leq i \leq n} ord(f_i),$$

where $ord(f_i)$ is the nonlinear order of $f_i(x)$. Theorem 1 means that the maximum nonlinear order of a APN permutation in $GF(2)^n$ is $n-1$. This upper bound is achievable (see Example 1 and 2, also Section 6). Theorem 6 tell us that any APN permutation must be depentent of all the quadratic terms, this may mean that the most important terms of a APN permutation are the quadratic ones.

3 The Nonlinearity of Permutations in $GF(2)^n$ and in $GF(2^n)$

If $f(x_1, \cdots, x_n) = (f_1(x), \cdots, f_n(x))$ is a permutation of $GF(2)^n$, let $B = \{\alpha_1, \cdots, \alpha_n\}$ be any basis of $GF(2^n)$ over $GF(2)$, then

$$F(X) = \sum_{i=1}^{n} f_i(x_1, \cdots, x_n)\alpha_i \tag{1}$$

is a permutation in $GF(2^n)$, and vice versa, where $X = \sum x_i\alpha_i \in GF(2^n)$. So there is an one-to-one correspondence between the permutations of $GF(2)^n$ and those of $GF(2^n)$ under a chosen basis of $GF(2^n)$ over $GF(2)$. We denote here and hereafter the permutation $f(x) = (f_1(x), \cdots, f_n(x))$ in (1) as $[F(X)]_B$.

For odd n, let $\{\alpha_1^*, \cdots, \alpha_n^*\}$ be the dual basis of B, then each component of $f(x)$ can be expressed as

$$f_i(x) = Tr(F(X)\alpha_i^*), \tag{2}$$

where $X = \sum x_i\alpha_i$.

The following result about the nonlinearity of the function $F(X)$ and $f(x)$ in (1) is obviously true, but is the theoretical foundation for constructing permutations in $GF(2)^n$ with good nonlinearity from those in $GF(2^n)$.

Theorem 7 *Let $B = \{\alpha_1, \cdots, \alpha_n\}$ be a basis of $GF(2^n)$ over $GF(2)$, $x = (x_1, \cdots, x_n)$, $y = (y_1, \cdots, y_n)$, $a = (a_1, \cdots, a_n)$, $b = (b_1, \cdots, b_n) \in GF(2)^n$, and $X = \sum x_i\alpha_i$, $Y = \sum y_i\alpha_i$, $A = \sum a_i\alpha_i$, $B = \sum b_i\alpha_i \in GF(2^n)$, then*
1) $P(F(X) + F(Y) = A \mid X + Y = B) = P(f(x) + f(y) = a \mid x + y = b)$;
2) $P_F(B) = P_f(b)$;
3) $P_F = P_f$;
4) $P_F = P_{F^{2^i}}$ for each integer i.

This theorem showes that the global and local nonlinearity of $F(X)$ and $f(x)$ is the same.

Theorem 8 *Let $f(x) = (f_1(x), \cdots, f_n(x))$ be a APN (DUD) permutation in $GF(2)^n$, then for each nonsingular $n \times n$ matrix A over $GF(2)$, $g(x) = (f_1(x), \cdots, f_n(x))A$ is also APN (DUD).*

The above Theorem 8 is useful in constructing APN permutations. Two permutations $f(x)$ and $g(x)$ in $GF(2)^n$ are said to be linearly equivalent if there are a nonsingular $n \times n$ matrix A over $GF(2)$ and a vector b in $GF(2)^n$ such that $f(x) = g(Ax + b)$.

Let $f(x) = [F(X)]_B$. For the changing of the basis, let $B' = \{\beta_1, \cdots, \beta_n\}$ be another basis of $GF(2^n)$ over $GF(2)$, $f'(x) = [F(X)]_{B'}$ and

$$(\beta_1, \cdots, \beta_n) = (\alpha_1, \cdots, \alpha_n)A^t, \tag{3}$$

then A is nonsingular and

$$f'(x) = (f_1(xA), \cdots, f_n(xA))A^{-1} \tag{4}$$

This result showes that the permutations deduced from a permutation in $GF(2^n)$ by changing the basis are usually not linear equivalent.

We now consider the conjugacy class of $Z_{2^n-1}^*$ mod (2^n-1). A conjugacy class C_k is the set $\{k2^i \bmod (2^n-1), i = 0, 1, \cdots,\}$. Theorem 7 tell us that $P_F = P_{F^{2^i}}$ for any permutations in $GF(2^n)$, so we can construct a class of permutations with good nonlinearity, provided that we can construct one.

It is well known that X^d is a permutation of $GF(2^n)$ iff $\gcd(d, 2^n-1) = 1$. In the following sections we investigate mainly the permutations X^d in $GF(2^n)$ with good nonlinearity. Before doing so, we need the following result about the nonlinear order of $[X^d]_B$, which was proved in [8] according to the citation of [7] (So we have deleted here our original proof).

Theorem 9 *Let B be a basis of $GF(2^n)$ over $GF(2)$, and d an integer, then $ord([X^d]_B) = W_H(d)$, where $W_H(d)$ is the Hamming weight of the binary representation of the integer d.*

4 Quadratic Permutations with Controllable Nonlinearity

In [5] Nyberg and Knudsen have studied the permutations f in $GF(2^m) = GF(2^d)^n$ which satisfy the property that every nonzero linear combination of the components of f is a balanced quadratic form x^tCx in n indeterminates over $GF(2^d)$ with $\mathrm{rank}(C + C^t) = n-1$. We now present a general result about the quadratic APN permutations.

Theorem 10 *Let $f(x) = (f_1, \cdots, f_n)$ be a permutation in $GF(2)^n$, where*

$$f_l(x) = \sum_{1 \le i < j \le n} a_{ij}^{(l)} x_i x_j + \sum_{i=1}^{n} b_i^{(l)} x_i + b_0^{(l)}, \quad 1 \le l \le n.$$

Setting the entries $a_{ij}^{(l)}$ of the matrix A_l as 0 when $i = j$, as $a_{\min\{i,j\}\max\{i,j\}}$ otherweise, then $f(x)$ is APN iff $rank(A_1w^t, \cdots, A_nw^t) = n-1$ for each $w \neq 0$.

Proof: Let

$$g_l(x, w) = f_l(x) + f_l(x+w) = xA_lw^t + \sum_{1 \le i < j \le n} a_{ij}^{(l)} w_i w_j + \sum_{i=1}^{n} b_i^{(l)} w_i$$

$$= xA_lw^t + f_l(w) + f_l(0).$$

For each $w \neq 0$, the set of linear equations

$$(g_1(x, w), \cdots, g_n(x, w)) = (d_1, \cdots, d_n) \neq 0 \tag{5}$$

has no solution or only two solutions iff $\text{rank}(A_1w^t, \cdots, A_nw^t) = n-1$ for each $w \neq 0$. This proves the theorem.

If we denote $f_l(x)$ as $f_l(x) = xC_lx^t + f_l(0)$, then $A_l = C_l + C_l^t$. Therefore the result presented here seems to be different from the one in [5]. From the forgoing proof it follows that the following Corollary 1 holds:

Corollary 1 *Let the symbols and notations as in Theorem 10. If*

$$\max_{w \neq 0} rank(A_1w^t, \cdots, A_nw^t) = k,$$

then $P_f \leq 2^{-k}$.

Theorem 11 *Let* $d = 2^l(2^k+1)$, $\gcd(d, 2^n-1) = 1$ *and* $m = \gcd(2^n-1, 2^k-1)$, B *be any basis of* $GF(2^n)$ *over* $GF(2)$, $f(x) = [X^d]_B$, *then* $P_f \leq (m+1)/2^n$.

Proof: Because of Theorem 7 it suffices to prove the case $d = 2^k + 1$. Let

$$G(X, \beta) = X^d + (X+\beta)^d = X^{2^k}\beta + X\beta^{2^k} + \beta^{2^k+1} = \alpha \tag{6}$$

Noticing that $G(X, \beta)$ is a linearized function of X, we need only to consider the number of solutions of the equation

$$\beta X^{2^k} + \beta^{2^k} X = 0, \tag{7}$$

which is equivalent to $X = 0$ and $(X\beta^{-1})^{2^k-1} = 1$.

Setting $H = \{x : x^u = 1, x \in GF(2^n)\}$, we see that H is a subgroup of the cyclic group $GF(2^n)^*$, so it is also cyclic, say $H = (h)$, then it is obvious that $h^m = 1$. Hence oder(h) divides m. It follows that the number of solutions of equation (7) is at most $m+1$, so is that of equation (6). This proves the theorem.

Corollary 2 *Let* $\gcd(2^k+1, 2^n-1) = 1$, *then the permutation* $[X^{2^l(2^k+1)}]_B$ *is APN iff* $\gcd(k, n) = 1$.

Proof: The permutation $[X^{2^l(2^k+1)}]_B$ is APN iff $m = \gcd(2^k-1, 2^n-1) = 1$, which is equivalent to $\gcd(k, n) = 1$.

For odd n the result of Corollary 2 has been proved in [5]. We get here a general result without requiring n being odd. On the other hand, it is apparent that $ord([X^{2^l(2^k+1)}]_B) = 2$.

5 A Class of Permutations of Order 3 with Good Nonlinearity

For a quadratic APN permutation $f = (f_1, \cdots, f_n)$ in $GF(2)^n$, it is not difficult to see that each $f_i(x)$ has a linear structure, i.e. , there is a vector w such that $f_i(x) + f_i(x+w) = f_i(w) + f_i(0)$. This may be a cryptographical demerit. In this sense it is important to construct permutations which have good nonlinearity and high nonlinear order. In this section we present a class of permutations of order 3 with good nonlinearity.

Theorem 12 *Let* $\gcd(3, 2^n - 1) = 1$, $d = 2^{i+2} + 2^{i+1} + 2^i$, *and* $i \geq 0$, B *a basis of* $GF(2^n)$ *over* $GF(2)$ *and* $f(x) = [X^d]_B$, *then* $ord(f) = 3$ *and* $P_f = 2^{1-n}$ *or* $3 * 2^{1-n}$.

Proof: Because of Theorem 7 and $d = 7 * 2^i$, it suffices to prove the case $d = 7$. Let

$$G(X, \beta) = X^d + (X + \beta)^d, \beta \neq 0, \tag{8}$$

then $G(X, \beta) = \alpha$ is equivalent to

$$Y^d + (Y + 1)^d = \gamma, \tag{9}$$

where $Y = X/\beta$, $\gamma = \alpha\beta^{-d}$. If $\gamma = 1$, then equation (9) is equivalent to $Y(Y^6 - 1) = 0$. Noticing that $\gcd(6, 2^n - 1) = \gcd(3, 2^n - 1) = 1$, so (9) has only two solutions.

If $\gamma \neq 0$, assume that (9) has two solutions in $GF(2^n)$, say Y_1, $1+Y_1$. Suppose it has another two solutions Y_2 and $1 + Y_2$ in $GF(2^n)$, let Y_3 and $1 + Y_3$ be the other two solutions of (9) in an extension field of $GF(2^n)$. By making use of the relationships between the cofficients and roots of equation (9), we get

$$Y_1 + Y_2 + Y_3 = 0 \text{ or } 1.$$

This means that $Y_3 \in GF(2^n)$. Whence $G(X, \beta) = \alpha$ has either no solution or two solutions or six solutions in $GF(2^n)$. This proves the first part of the theorem. Finally, it follows from Theorem 9 that $\text{ord}(f) = 3$.

In the following sections we will see that permutation $[X^7]_B$ of $GF(2)^5$ is APN. We now discuss when the $f(x)$ in Theorem 12 is APN. If (9) has more then two solutions in $GF(2^n)$, then it follows from the above proof that it has six solutions, say, Y_1, $1+Y_1$, Y_2, $1+Y_2$, Y_3, $1+Y_3$. By making use of the relations between the cofficients and roots of equation (9), we get

$$\begin{cases} (Y_1^2 + Y_1)^2 + (Y_2^2 + Y_2)^2 + (Y_1^2 + Y_1)(Y_2^2 + Y_2) = 1 \\ (Y_1^2 + Y_1)(Y_2^2 + Y_2)(Y_2^2 + Y_2 + Y_1^2 + Y_1) = r + 1 \end{cases}$$

Let $Y_1^2 + Y_1 = a$, $Y_2^2 + Y_2 = b$, then a, $b \in GF(2^n)$. Whence we obtain

$$\begin{cases} a^2 + b^2 + ab = 1 \\ ab(a + b) = r + 1, \end{cases}$$

which is equivalent to

$$\begin{cases} b^3 + b + r + 1 = 0 \\ a^3 + a + r + 1 = 0 \\ (a + b)^3 + a + b + r + 1 = 0, \end{cases}$$

because a, $b \neq 0$. This means that the equation

$$X^3 + X + r + 1 = 0 \tag{10}$$

has three solutions in $GF(2^n)$.

On the other hand, let

$$x^3 + X + r + 1 = (X + a)(X^2 + aX + c),$$

then we have

$$\begin{cases} a^2 + c = 1 \\ ac = r + 1. \end{cases}$$

Since $X^2 + aX + a^2 + 1 = a^2[(X/a)^2 + (X/a) + (a^2 + 1)/a^2]$ and it is known that polynomial $Y^2 + Y + d$ is reducible in $GF(2^n)$ iff $Tr(a) = Tr(a^{-1})$, where $d \in GF(2^n)$. Therefore $X^3+X+r+1$ has only one solution a iff $Tr(a) = Tr(a^{-1})$. Thus, if we can give a condition such that $\gcd(3, 2^n - 1) = 1$ and every solution Y of equation (9) satisfies $Tr(Y) = Tr(Y^{-1})$ in $GF(2^n)$, then the permutation f in Theorem 12 must be APN.

6 A Class of APN Permutations of Order $n-1$ in $GF(2)^n$

It has been already been mentioned that constructing higher order permutations with good nonlinearity is cryptographically desirable. In this section we present a class of maximum order permutations in $GF(2)^n$.

Theorem 13 *Let* $\gcd(3, 2^n - 1) = 1$ *and* $d = 2^n - 2^i - 1$, $0 \le i \le n - 1$, B *a basis of* $GF(2^n)$ *over* $GF(2)$. *Then* $f(x) = [X^d]_B$ *is a maximum order APN permutation in* $GF(2)^n$.

Proof: We first consider the case $i = 0$. Then $F(X) = X^d = 0$ when $X = 0$, $F(X) = X^{-1}$ otherweise. Now we discuss the number of solutions of the equation

$$X^d + (X + \beta)^d = \alpha \tag{11}$$

If $\alpha = \beta^d$, then 0 and β are two solutions of (11) in $GF(2^n)$. Suppose that $X \neq 0, \beta$, is another solution of (11) in $GF(2^n)$, then we get from (11) that

$$X^2 + \beta X + \beta^2 = 0. \tag{12}$$

It follows that $X^3 = \beta^3$, which gives $X = \beta$, because that $\gcd(3, 2^n - 1) = 1$. A contridiction. Hence, in this case (11) has only two solutions.

If $\alpha \neq \beta^d$, then (11) has no solutions 0 and β. Whence (11) can be written as

$$G(X, \beta) = X^{-1} + (X + \beta)^{-1} = \beta / X(X + \beta) = \alpha, \tag{13}$$

which is equivalent to

$$X^2 + \beta X + \alpha^{-1}\beta = 0. \tag{14}$$

Obviously, (14) has at most two solutions for each $\alpha \neq \beta^d$, so has equation (13).

Summarizing the above results, we see that $[X^d]_B$ is APN. Noticing that $d = 2^n - 2$, we get $W_H(d) = n - 1$. Whence $\mathrm{ord}(f) = n - 1$. Finally, it follows from Theorem 7 that for each $d = 2^n - 1 - 2^i$, the conclusion of the theorem is true.

7 A Class of Permutaions of Order $n - 2$ in $GF(2)^n$ with Good Nonlinearity

This section presents a class of permutations of order $n-2$ in $GF(2)$ with good nonlinearity.

Theorem 14 *Let* $\gcd(3, 2^n - 1) = 1$, $\gcd(7, 2^n - 1) = 1$ *and* $d = 2^n - 2^{i+1} - 2^i - 1$, $0 \leq i \leq n-2$. *Then the permutation* $f(x) = [X^d]_B$ *has order n-2 and nonlinearity* $P_f = 2^{1-n}$ *or* $3 * 2^{1-n}$.

Proof: Because of Theorem 7 it suffices to prove the case $d = 2^n - 1 - 3$. Consider now the equation

$$G(X, \beta) = X^d + (X + \beta)^d = \alpha, \ \alpha \neq \beta^d, 0. \tag{15}$$

Apparently, (15) has no solutions 0 and β. Therefore (15) is equivalent to

$$X^6 + X^5\beta + X^4\beta^2 + X^3\beta^3 + X^2\alpha^{-1}\beta + X\alpha^{-1}\beta^2 + \alpha^{-1}\beta^3 = 0. \tag{16}$$

Similar to the proof of Theorem 12, we can prove that (15) has either no solution or two or six solutions in $GF(2^n)$.

What remains to be consided, is the equation

$$X^d + (X + \beta)^d = \beta^d. \tag{17}$$

Let $Y = X/\beta$, then (17) is equivalent to

$$Y^d + (1 + Y)^d = 1. \tag{18}$$

We conclude that (18) has only two solutions 0 and 1 in $GF(2^n)$. If not so, say that $Y_1 \neq 0, 1$, is another one in $GF(2^n)$. Then we get

$$1 + Y_1 + Y_1^2 + Y_1^3 + Y_1^4 + Y_1^5 + Y_1^6 = 0. \tag{19}$$

Whence $Y_1^7 = 1$. It follows that $Y_1 = 1$, a contridiction. Hence (18) has only two solutions in $GF(2^n)$.

By summarizing the above results, we see that $P_f = 2^{1-n}$ or $3 * 2^{1-n}$. It can be easily seen that $\mathrm{ord}(f)=n-2$.

8 On the Nonlinearity of the Permutations X^d in $GF(2^n)$ with $d = 2^m - 1$

For $d = 2^m + 1$ with $\gcd(m, n) = 1$, we have seen that X^d is APN in $GF(2^n)$. It is natural to ask whether the permutation X^{2^m-1} is APN. A simple example is that x^7 is APN in $GF(2^5)$, but not APN in $GF(2^4)$. Therefore X^{2^m-1} may be APN or not in $GF(2^n)$, it depents on the structure of the field $GF(2^n)$. To investigate the problem further. We need the following lemma:

Lemma 2 *Assume that n and $2^n - 1$ are two primes, then each nonzero conjugacy class of $Z^*_{2^n-1} mod(2^n - 1)$ has n elements, and there are $(2^n - 2)/n$ such conjugacy classes.*

Since $d = 2^m - 1$, we get

$$G(X, \beta) = X^d + (X + \beta)^d = \beta^d(Y^d + 1)/(Y + 1),\ X \neq \beta,$$

where $Y = X/\beta$. Therefore we need only to discuss the number of solutions of the equation

$$Y^{2^m-1} + 1 = r(Y + 1),\ r \neq 0,\ 1. \tag{20}$$

For the solutions of (20), we have the following conjecture:

Conjecture 1 *Assume that n and $2^n - 1$ are two primes, then for each $2 \leq i \leq n - 1$, equation (20) has at most two solutions other then 1 in $GF(2^n)$.*

In the case $m = n - 1$, the conclusion has already been proved in Theorem 13. If the conjecture is true, then every permutation $[X^{2^m-1}]_B (2 \leq m \leq n - 1)$ is APN in $GF(2)^n$.

9 Summary and Remarks

In this paper basic properties of APN permutations are presented. These results are useful in seeing the nature of the APN permutations and in constructing these permutations. By investigating mainly the permutations X^d in $GF(2^n)$, several classes of permutations in $GF(2)^n$ with good nonlinearity have been obtained. Some of them have high nonlinear order.

Included here are also three kinds of methods for constructing APN permutations in $GF(2)^n$. 1) Matrix Method: From an APN permutation $f = (f_1, \cdots, f_n)$ by multiplying a $n \times n$ nonsingular matrix A over $GF(2)$ to obtain another APN permutation $g(x) = (f_1, \cdots, f_n)A$; 2) Conjugacy Method: From a APN permutation $F(X)$ in $GF(2^n)$ to get $G(X) = F(X)^{2^i} = F(X^{2^i})$; 3) Basis Method: From a APN permutation $F(X)$ in $GF(2^n)$ to obtain different $[F(X)]_B$, by changing the basis B of $GF(2^n)$ over $GF(2)$.

After the simultaneous submissions of this paper and [7], we have found some

overlaps between them, which should be made clear. Theorem 11 in this paper is an overlap with the first part of Proposition 3 in [7], and Theorem 13 here is a special case of of Proposition 6 in [7].

During Eurocrypt'93 Dr Nyberg has made some comments and suggestions for this paper. One is that the condition $\gcd(3, 2^n - 1) = 1$ in Theorem 12 and 13 is actually that n is odd. Another suggestion of Nyberg is a generalized definition of the linear equivalence for permutations, by which two permutations f and g over a field F are said to be linearly equivalent if there are two affine permutations A and B such that $f = B \circ g \circ A$, here $\circ$ denotes the composition operation of functions. By this definition all the functions x^d's for d's in the same conjugacy class are linearly equivalent.

Acknowlegements: The authors would like to thank Dr. Nyberg for the above helpful comments and suggestions, and the referees for pointing out a necessary condition of Corollary 2 and some typos of the original paper.

References

[1] E. Biham, A. Shamir. *Differential Cryptanalysis of DES-like Cryptosystems.* Advances in Cryptology, Proceedings of Crypt'90, Springer-Verlag, 1990.

[2] E. Biham, A. Shamir. *Differential Cryptanalysis of Snefru, Khafre, Redoc-II, Lokl and Lucifer.* Crypto'91, LNCS Vol.576, Springer-Verlag, 1991, pp.156-171.

[3] D. Chaum, J.H. Evertse. *Cryptanalysis of DES with a reduced number of rounds.* Advances in Cryptology, Proceedings of Crypto'85, Springer-Verlag, 1986, pp.192-211.

[4] X. Lai, J.L.Massey, S. Murphy. *Markov Ciphers and Differential Cryptanalysis.* Advances in Cryptology, Eurocrypto'91, LNCS Vol.547, Springer-Verlag, 1991, pp.17-38.

[5] K. Nyberg, L.R. Knudsen. *Provable Security against Differential Cryptanalysis.* Advances in Cryptology, Crypto'92.

[6] J. Pieprzyk. *Nonlinearity of Exponent Permutations*, Advances in Cryptology, Proc. Eurocrypt'89, Springer-Verlag, 1990.

[7] K. Nyberg. *Differentially uniform mappings for cryptography,* Eurocrypt'93, this proceedings.

[8] C. Carlet. *Codes de Reed-Muller, Codes de kerdock et de Preparata,* thesis, Publication of LITP, Institut Blaise Pascal, Université Paris 6, 90.59 (1990).