Binomial differentially 4 uniform permutations with high nonlinearity

Carl Bracken\textsuperscript{a}, Chik How Tan\textsuperscript{b,1}, Yin Tan\textsuperscript{b,*,1}

\textsuperscript{a} Department of Mathematics, School of Physical & Mathematical Sciences, Nanyang Technology University, Singapore
\textsuperscript{b} Temasek Laboratories, National University of Singapore, 117411 Singapore

\textbf{Article info}

\textbf{Article history:}
Received 19 April 2011
Revised 22 November 2011
Accepted 25 November 2011
Available online 9 December 2011
Communicated by Gary McGuire

\textbf{MSC:}
94A60
11T71
14G50

\textbf{Keywords:}
APN function
Differentially 4 uniform function
Permutation polynomial
Quadratic function

\textbf{Abstract}

Differentially 4 uniform permutations with high nonlinearity on fields of even degree are crucial to the design of S-boxes in many symmetric cryptographic algorithms. Until now, there are not many known such functions and all functions known are power functions. In this paper, we construct the first class of binomial differentially 4 uniform permutations with high nonlinearity on $\mathbb{F}_{2^m}$, where $m$ is an odd integer. This result gives a positive answer to an open problem proposed in Bracken and Leander (2010) [7].

© 2011 Elsevier Inc. All rights reserved.

1. Introduction

Many symmetric cryptosystems use S-boxes to provide nonlinear functions in cipher algorithm. Such S-boxes are functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. These functions should have low differential uniformity and highly nonlinearity so that it is resistant to differential [3] and linear [15] attacks respectively. Moreover, it is often crucial to require these functions to be permutations and, for software implementation, to be defined on a field with even degree ($n$ is even). The well-known AES (Advanced Encryption Standard) uses the inverse function which is a differential 4 uniform permuting power mapping.

* Corresponding author.

E-mail addresses: carlbracken@ntu.edu.sg (C. Bracken), tsltch@nus.edu.sg (C.H. Tan), itanyinmath@gmail.com (Y. Tan).

\textsuperscript{1} The work was funded by DSO National Laboratories, Singapore.

1071-5797/$ – see front matter © 2011 Elsevier Inc. All rights reserved.
Usually we have the following two methods to characterise the nonlinear property of a function \( F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n} \). For any \( a \in \mathbb{F}_{2^n}^* (\equiv \mathbb{F}_{2^n} \setminus \{0\}) \) and \( b \in \mathbb{F}_{2^n}^* \), define
\[
\delta_F(a, b) = |\{ x : x \in \mathbb{F}_{2^n} : F(x + a) + F(x) = b \}|.
\]
The multiset \( \{\delta_F(a, b) : a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}^*\} \) is called the differential spectrum of \( F \). In order to be resistant against differential attacks, the differential uniformity
\[
\Delta_F \triangleq \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}^*} \delta_F(a, b)
\]
should be as small as possible. It is well known that, for fields with even characteristic, the lowest possible uniformity is 2 and functions with this property are called almost perfect nonlinear (APN) functions. Recently, several families of APN functions were found (see \([2,5,6,8,9]\) and the references there), most of which are quadratic functions. They are demonstrated or conjectured to be EA- or CCZ-inequivalent to the known APN power functions. However, there are no known APN permutations on the fields of even degree except a sporadic example on \( \mathbb{F}_{2^6} \) found by Dillon \([11]\). The existence of APN permutations on other fields of even degree remains an important problem. Therefore, a natural method to fulfill the design of S-boxes is to find differentially 4 uniform permutations.

Before discussing differentially 4 uniform permutations, we first introduce the second concept of nonlinearity. For a function \( F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n} \), the Walsh (Fourier) transform \( F^W : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}^* \rightarrow \mathbb{C} \) of \( F \) is defined as:
\[
F^W(a, b) := \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(ax + bF(x))}, \quad a \in \mathbb{F}_{2^n}, \ b \in \mathbb{F}_{2^n}^*.
\]
where \( Tr \) denotes the usual trace function. The set \( W_F := \{ F^W(a, b) : a \in \mathbb{F}_{2^n}, \ b \in \mathbb{F}_{2^n}^*\} \) is called the Walsh spectrum of \( F \). The nonlinearity \( NL(F) \) of \( F \) is defined as
\[
NL(F) \triangleq 2^{n-1} - \frac{1}{2} \max_{x \in W_F} |x|.
\]
It is known that if \( n \) is odd, the nonlinearity \( NL(F) \) is upper-bounded by \( 2^{n-1} - 2^{n-2} \); and when \( n \) is even it is conjectured that \( NL(F) \) is upper-bounded by \( 2^{n-1} - 2^{n/2} \). We call functions highly (maximal) nonlinear if their nonlinearity attains these bounds.

Highly nonlinear power mappings that are permutations have been studied systematically, see \([12]\) and the references there. It is conjectured that all such mappings have been found. As pointed out by Carlet \([10]\), the alternatives for the inverse function are very rare and it is a main challenge to find more candidates for good S-boxes. Recently, the function (VII) in \([12, p. 142]\) is proven to be a differentially 4 uniform highly nonlinear permutation in \([7]\). Unfortunately, by using a computer, we test the remaining power functions in \([12, p. 142]\) and do not find new differentially 4 uniform permutations. From \([7, Table 1]\), we can see that the list of highly nonlinear differentially 4 uniform permutations on fields of even degree is still limited. The known such functions are Gold, Kasami, Inverse functions and the one in \([7]\). This motivates us to find more functions with these properties. This problem is also proposed as an open problem in \([7]\).

In this paper, we prove the function in the following theorem is a highly nonlinear differentially 4 uniform permutation. It is obtained, by changing certain conditions, from a recently found APN function in \([8]\).

**Theorem 1.1.** Let \( n = 3k \) and \( k \) is an even integer with \( 3 \nmid k, k/2 \) is odd. Let \( s \) be an integer with \( \gcd(3k, s) = 2 \) and \( 3 \mid k + s \). Define the function \( F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n} \).
\[ F(x) = \alpha x^{2^i+1} + \alpha^2 x^{2^k+k^i+2^{k+s}}, \]  

where \( \alpha \) is a primitive element of \( \mathbb{F}_{2^n} \). Then \( F \) is a differentially 4 uniform permutation. Moreover, the Walsh spectrum of \( F \) is a subset of \( \{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\} \). Therefore, \( F \) is a highly nonlinear function.

More generally, using a similar argument as the one in this paper, we may show that the function \( G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \) defined by

\[ G(x) = \alpha x^{2^i+1} + \alpha^2 x^{2^k+k^i+2^{k+s}}, \]

where \( 3 \nmid k, k/2 \) is odd, \( \gcd(3k, s) = 2 \), \( i \equiv ks \mod 3 \), \( t \equiv -i \mod 3 \) is a differentially 4 uniform permutation and the Walsh spectrum is a subset of \( \{0, \pm 2^{3k/2}, \pm 2^{(3k+2)/2} \} \). It is easy to see that the function \( F \) in Theorem 1.2 is the particular case \( i \equiv 2 \mod 3 \). Moreover, we may demonstrate the case \( i \equiv 1 \mod 3 \) can be transformed easily from the other case.

We should mention not all known APN functions could derive differentially 4 uniform permutations using the method above. After studying the quadratic APN functions listed in [6], by using MAMGA, we find only two classes of functions could be highly nonlinear differentially 4 uniform permutations, the one in Theorem 1.2 and the one in Problem 5.1. Unfortunately, we cannot prove the latter one and state it as an open problem.

To obtain more general results, we will prove the following theorem and then Theorem 1.1 can be seen as a corollary.

**Theorem 1.2.** Let \( n = 3k \) and \( t \) is a divisor of \( k \) with \( 3 \nmid k, k/2 \) is odd. Let \( s \) be an integer with \( \gcd(3k, s) = t \), \( 3 \nmid k + s \). Define the function \( F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \)

\[ F(x) = \alpha x^{2^i+1} + \alpha^2 x^{2^k+k^i+2^{k+s}}, \]

where \( \alpha \) is a primitive element of \( \mathbb{F}_{2^n} \). Then \( F \) is a differentially \( 2^t \) uniform permutation and the differential spectrum of \( F \) is \( \{0, 2^t\} \). Moreover, for any \( a, b \in \mathbb{F}_{2^n} \), \( |F^W(a, b)| \leq 2^{(n+t)/2} \) if \( n+t \) is even, and \( |F^W(a, b)| \leq 2^{(n+t-1)/2} \) if \( n+t \) is odd.

In the next three sections, we will prove the function \( F \) in Theorem 1.2 is a permutation, differentially \( 2^t \) uniform and determine its Walsh spectrum. Some remarks and an open problem are given in Section 5.

### 2. \( F \) is a permutation

We will prove the function \( F \) is a permutation in this section. A more general result is given to obtain necessary and sufficient condition for the function \( F \) of the form (1) being a permutation. The proof is similar to the one in [8, Proposition 1] and we only give a sketch with just minor changes.

**Lemma 2.1.** Let \( k \) be an integer with \( 3 \nmid k \) and \( s \) be an integer with \( \gcd(3k, s) = t \), \( 3 \nmid k + s \). Then the function \( F(x) = \alpha x^{2^i+1} + \alpha^2 x^{2^k+k^i+2^{k+s}} \) is a permutation if and only if \( k/t \) is odd.

**Proof.** If \( k/t \) is even, then \( s/t, (2k+s)/t \) are odd. Indeed, clearly we have \( \gcd(k, s) = \gcd(2k+s, k) = t \) and then \( \gcd(k/t, s/t) = \gcd((2k+s)/t, k/t) = 1 \). It follows from \( k/t \) is even that \( s/t \) and \( (2k+s)/t \) are both odd. Now, as \( 2^t + 1 \) \( \nmid 2^t+1 \) if and only if \( i \mid j \) and \( j/i \) is odd, we have \( 2^t + 1 \mid 2^t+1, 2^t + 1 \mid 2^{2k+s}+1 \). Obviously there exists an element \( y \in \mathbb{F}_{2^n} \) with order \( 2^t+1 \), we have \( F(\gamma x) = F(x) \) for all \( x \in \mathbb{F}_{2^n} \). Therefore, \( F \) is not a permutation.

Next, we prove \( F \) is a permutation when \( k/t \) is odd. To prove \( F \) is a permutation, it is equivalent to show the function \( F/\alpha \) is so. By abuse of notation, we still denote \( F/\alpha \) by \( F \). We need to show that the equation \( F(x + v) + F(x) = 0 \) has no solution for every nonzero \( v \in \mathbb{F}_{2^n} \). Now
\[ \Delta_v(x) = F(x) + F(x + \nu) = v^{2^s+1} \left( \left( \frac{x}{v} \right)^{2^s} + \left( \frac{x}{v} \right) \right) + v^{2^s+1} + \alpha \cdot \frac{\nu}{\Delta_1} v^{2^s+2^k-s} \left( \left( \frac{x}{v} \right)^{2^k} + \left( \frac{x}{v} \right)^{2^k+s} \right) + \alpha \cdot \frac{\nu}{\Delta_1} v^{2^s+2^k+s}. \]

After replacing \( x \) by \( vx \) and divide by \( v^{2^s+1} \) we have

\[ \Delta_v(x) = a(x^{2^k} + x^{2^k+s} + 1) + x^{2^s} + x + 1, \]

where \( a = (\alpha v^{2^k+2^k+1})^{2^k-1} \). Clearly \( a \notin F_2 \). Otherwise, assume that \( a = (\alpha v^{2^k+2^k+1})^{2^k-1} \). On the one hand, since \( 3 \mid k \), the left-hand side is not a 7-th power. On the other hand, it follows from \( 3 \mid k - s, \ 3 \mid s \) that \( 3 \mid 2^k + 2^s + 1 \), i.e., the right-hand side is a 7-th power. This obtains the contradiction. Now, denote by \( y = x^{2^k}, z = y^{2^k}, b = a^{2^k} \), \( c = b^{2^k} \), the equation \( \Delta_v(x) = 0 \) can be written as

\[ a(z + y^{2^s} + 1) + (x^{2^s} + x + 1) = 0. \]

Consider the conjugated equations we have the following system of equations:

\[ f_1 = a(z + y^{2^s} + 1) + (x^{2^s} + x + 1) = 0, \]
\[ f_2 = b(x + z^{2^s} + 1) + (y^{2^s} + y + 1) = 0, \]
\[ f_3 = \frac{1}{ab}(y + x^{2^s} + 1) + (z^{2^s} + z + 1) = 0. \]

Using the computations as the ones in [8, Proposition 1], we obtain

\[ 0 = F(x + \nu) + F(x) = P(a)\nu(x^{2^s} + x + 1), \]

where

\[ P(a) = \frac{1}{a^{2^s+1}} \left( a^{2^s+1} + 1 \right) + a^{2^s+1} + a^{2^s+2^k} + a^{2^s} + a^{1+2^k} + a^{2^k}. \]

Assuming \( P(a) \neq 0 \) for all nonzero \( a \in F_2 \), then \( x^{2^s} + x + 1 = 0 \) and substituting \( x^{2^s} = x \) which is equivalent to \( x \in F_{2\gcd(2s,3k)} = F_{2\gcd(3,3k)} = F_{2^s} = F_{2^s} \cap F_{2^s} \). Then \( x^{2^s} + x + 1 = 1 \neq 0 \). Now, the last remaining to prove is that \( P(a) \neq 0 \) for all \( a = (\alpha v^{2^k+2^k+1})^{2^k-1} \) (note that \( a \notin F_2 \)). Otherwise,

\[ a = \left( \frac{a + 1}{c + 1} \right)^{2^s+1} \left( \frac{b + 1}{a + 1} \right)^{2^s+1} \left( \frac{a + 1}{c + 1} \right)^{2^s+1}, \]

which follows that

\[ \alpha^{2^k-1} = \left( \frac{a + 1}{c + 1} \right)^{2^s+2^s+1}. \]
Since \(3 \mid k + s\) and \(3 \mid s\), we have \(7 \mid 2^k + 2^s + 1\) (use the fact \(2^r \equiv 2, 4 \mod 7\) when \(r \equiv 1, 2 \mod 3\) respectively). Therefore, the left-hand side of the above is not a 7-th power, while the right-hand side is, a contradiction. We complete the proof. \(\square\)

3. **F is differentially \(2^t\) uniform**

In this section, we will prove \(F\) is a differentially 4 uniform function. The method used here gives another proof of the function \(F\) being an APN function when \(\gcd(3k, s) = 1\).

**Lemma 3.1.** Let \(F\) be the function defined in Theorem 1.2. Then \(F\) is a differentially \(2^t\) uniform function. Moreover, the differential spectrum of \(F\) is \(\{0, 2^t\}\).

**Proof.** Now \(F(x) = \alpha x^{2^k+1} + \alpha^2 x^{2^{k+s}+2^{k+s}}\). We need to show that, \(\Delta_0(x) = \alpha F(x) + \alpha F(x + a) + \alpha F(a) = 0\) has 0 or \(2^t\) solutions for any nonzero \(a\), with the given conditions on \(s\) and \(k\). Expanding the above equation and replacing \(x\) with \(xa\) we get

\[
\alpha a^{2^k+1} (x + x^2) + \alpha^2 a^{2^{k+s}+2^{k+s}} (x^2 - x) = 0. \tag{3}
\]

Next, we rearrange terms and multiply across by \(\alpha^{2^{k-s}} a^{2^{k+s}}\) to obtain

\[
\alpha^{2^k+1} a^{2^{k+s}+2^{k+s}} \alpha a^{2^k} x^{2^k} = \alpha^{2^k+1} a^{2^{k+s}+2^{k+s}} \alpha a^{2^k} x^{2^k}.
\tag{4}
\]

Denoting \(\text{Tr}_k\) by the relative trace map from \(\mathbb{F}_{2^{3k}} \rightarrow \mathbb{F}_{2^k}\), i.e., \(\text{Tr}_k(y) = y + y^{2^k} + y^{2^k}\), we apply this trace map to Eq. (2). Noting that \(\text{Tr}_k(y + y^{2^k}) = 0\) for all \(y \in \mathbb{F}_{2^{3k}}\) we see that the left-hand side of (4) vanishes yielding the expression

\[
\text{Tr}_k(\alpha^{2^k+1} a^{2^{k+s}+2^{k+s}} + \alpha^{2^k+2^{k+s}+2^{k+s}} a^{2^{k+s}+2^{k+s}+2^{k+s}} x^{2^k}) = 0.
\]

This implies

\[
\text{Tr}_k \left( (\alpha^{2^k+1} a^{2^{k+s}+2^{k+s}} + \alpha^{2^k+2^{k+s}} a^{2^{k+s}+2^{k+s}+2^{k+s}} x^{2^k}) \right) = 0.
\]

We now write this as

\[
Ax + A^2 x^{2^k} + A^{2^{k+s}} x^{2^k} = 0, \tag{5}
\]

where \(A = \alpha^{2^{k-s}+2^{k-s}+2^{k+s}} a^{2^{k-s}+2^{k+s}+2^{k+s}}\). Here we claim \(A \neq 0\). Otherwise, we have

\[
\alpha^{2^k+1} a^{2^{k+s}+2^{k+s}+2^{k+s}+2^{k+s}} = \alpha^{2^{k-s}+2^{k-s}+2^{k+s}+2^{k+s}}.
\]

After rearranging we have \(\alpha^{2^{k+s}+1} = \alpha^{2^{k-s}+1} a^{2^{k-s}} (2^k-1)(2^{k+s}-1)\). Notice that \(3 \mid k + s\) and then left-hand side of the above identity is a 7-th power, while the right-hand side is not as \(\alpha^{2^{k-s}-1}\) is not a 7-th power. Returning to (3), we now multiply across by \(a^{2^k}\) and apply the relative trace map. In this instance it is the other two terms that vanish and this gives the following equation

\[
Bx + B^{2^k} x^{2^k} + B^{2^{k+s}} x^{2^k} = 0, \tag{6}
\]
where \( B = \alpha a^{2k+2^k+1} + \alpha 2^{-k} a^{2^{k+3}+2^{k+1}} \). Similar arguments may show \( B \neq 0 \). We combine (5) and (6) to obtain

\[
(AB^{2^k} + A^{2^k} B)x + \left(A^{2^k} B^{2^k} + A^{2^{k+1}} B^2\right)x^2 = 0.
\]

Routine calculations confirm that \( AB^{2^k} + A^{2^k} B = A^{2k} B^{2^k} + A^{2^{k+1}} B^2 \), hence we have shown that \( x = x^2 \), provided \( AB^{2^k} + A^{2^k} B \neq 0 \). Let \( \phi = \alpha a^{2k+2^k} + \alpha 2^{-k} a^{2^{k+3}+2^{k+1}} \). It can verified that \( A = \alpha a^{2^{-k}} \alpha \phi^{2^{-k}} \) and \( B = \alpha \phi \). Now if \( AB^{2^k} + A^{2^k} B = 0 \), substituting \( A, B \), rearranging terms and taking \( 2^t \)-th power we have \( \alpha^{2^{-k} - 1} = (\alpha a(1-2^{-k})(2^{k+1}-1) \). Clearly the right-hand side is a 7-th power, while the left-hand side is not. Now, again we return to (3) and using the fact that \( x \in \mathbb{F}_2^* \) we now have,

\[
(\alpha a^{2^k+1} + \alpha a 2^{-k} a^{2^{k+1}+1} + x^2) = 0. \tag{7}
\]

Obviously \( \alpha a^{2^k+1} + \alpha 2^{-k} a^{2^{k+1}+1} \neq 0 \). Otherwise, it follows from \( \alpha^{2^k-1} = a^{(2^k-1)(2^k+1)} \) that the left-hand side is not a 7-th power, while the right-hand side is. Therefore, (7) implies that \( x \) can only take 0 or 2 values as \( \text{gcd}(s, 3k) = t \) and we are done. \( \square \)

4. \( F \) is highly nonlinear

In this section, we will determine the nonlinearity of \( F \), First, we give a well-known result which will be used later. A proof can be found in [4, Corollary 1].

**Lemma 4.1.** Let \( d, s \) be positive integers satisfying \( \text{gcd}(n, s) = 1 \) and let \( G(x) = \sum_{i=0}^{d} t_i x^{2^i} \in \mathbb{F}_2^n[x] \). Then the equation \( G(x) = 0 \) has at most \( 2^d \) solutions.

**Lemma 4.2.** Let \( F \) be the function defined in Theorem 1.2. Then for any \( a, b \in \mathbb{F}_2^s \), \( F^{W}(a, b) \leq 2^{(n+t)/2} \) if \( n + t \) is even and \( F^{W}(a, b) \leq 2^{(n-t-1)/2} \) if \( n + t \) is odd.

**Proof.** Clearly the Walsh spectrum of \( F \) is the same as the function \( F/\alpha \). By abuse of notation, we denote \( F/\alpha \) by \( F \) and \( w = \alpha^{2^k-1} \). For any \( a \in \mathbb{F}_2^s, b \in \mathbb{F}_2^t \), the Walsh spectrum of \( F \) is

\[
F^{W}(a, b) = \sum_{x \in \mathbb{F}_2^s} (-1)^{\text{Tr}(ax + bF(x))}.
\]

Squaring \( F^{W}(a, b) \) gives

\[
F^{W}(a, b)^2 = \sum_{x \in \mathbb{F}_2^s} \left( \sum_{y \in \mathbb{F}_2^s} (-1)^{\text{Tr}(ax + bF(x) + ay + bF(y))} \right) = \sum_{x \in \mathbb{F}_2^s} \left( \sum_{u \in \mathbb{F}_2^t} (-1)^{\text{Tr}(ax + bF(x) + a(x+u) + bF(x+u))} \right).
\]

Now

\[
F^{W}(a, b)^2 = \sum_{u} (-1)^{\text{Tr}(wu + bu^{2^k+1} + bw^{2^{k+1}} + 2^{k+s})} \sum_{x} (-1)^{\text{Tr}(xu)} L_b(u),
\]

where \( L_b(u) = bu^{2^s} + (bu)^{2^s} + (bw)^{2^{k}} u^{2^{k+1}} + (bw)^{2^{k+1}} u^{2^{k+s}} \). Since \( \sum_{x} (-1)^{\text{Tr}(xu)} = 0 \) when \( c \neq 0 \) and \( 2^t \) otherwise, so
\[ F^W(a, b)^2 = 2^n \sum_{u \in K} (-1)^{\text{Tr}(au + bu^{2^{s+1} + bwu^{2^{-k} + 2^k + s})}, \]

where \( K \) is the kernel of \( L_b(u) \). Now if we can show that the size of the kernel is at most \( 2^t \), then clearly

\[ 0 \leq \sum_{u \in K} (-1)^{\text{Tr}(au + bu^{2^{s+1} + bwu^{2^{-k} + 2^k + s})} \leq 2^t. \]

Hence, \( F^W(a, b) \leq 2^{(n+1)/2} \) if \( n + t \) is even and \( F^W(a, b) \leq 2^{(n+t-1)/2} \) if \( n + t \) is odd as \( F^W(a, b) \) is an integer.

In the following we will prove \( |K| \leq 2^t \). We consider the two expressions

\[
(bw)^{-2^k}L_b(u) + b^{1-2^k-2^{-k}}wL_b(u)^{2^k} + b^{-2^k}L_b(u)^{2^k} = 0, \\
b^{-2^{-s}}L_b(u) + b^{2^{-k-s}-2^{-k-s}-2^{-s}}w^{2^{-k-s}}L_b(u)^{2^k} + b^{-2^{k-s}}w^{-2^{k-s}}L_b(u)^{2^k} = 0.
\]

From these we obtain

\[
\begin{align*}
(b^{2^{s-2^k}}w^{2^k} + b^{2^{k-s-2^k}}w^{2^{k-s}})u^{2^{-s}} & + (bw)^{2^{k-s}-2^k + b^{2^{k-s}+1-2^k-2^k}w)u^{2^{k-s}} \\
 & + (b^{2^{-s}+1-2^k-2^k}w^{2^{-s}+1} + b^{2^{-k-s}-2^{-k-s}})u^{2^{-k-s}} = 0, \\
(b^{1-2^{-s}} + b^{2^{-k-s}+2^{-k-s}-2^{-k-s}}w^{2^{-k-s}+2^{-k-s}})u^{2^s} & + (b^{2^{-k-s}+2^{-2^{-s}-2^{-k-s}}w^{2^{-k-s}+2^{-k-s}}})u^{2^{k+s}} \\
 & + (b^{2^{-s}}w^{2^k} + b^{2^{-k-s}}w^{2^{-k-s}+2^{-k-s}})u^{2^{-2^{-k-s}}}. \tag{8}
\end{align*}
\]

Assume the coefficient \( b^{2^{s-2^k}}w^{2^k} + b^{2^{k-s-2^k}}w^{2^{k-s}} = 0 \), then \( w^{2^{k-s}+2^k} = b^{-2^{k-s}+2^{-k-s}-2^{-k-s}}. \) Taking \( 2^{-k} \)-th power on both sides and replacing \( w \) with \( \alpha^{2^k-1} \) we have

\[ \alpha^{(2^k-1)(2^{s+1})} = b^{(2^{k-1}+1)(2^{-s}-2^{-k-s})}. \tag{10} \]

Clearly the right-hand side of (10) is a 7-th power, while the left-hand side is not. Similar arguments may show the remaining coefficients are nonzero and we omit them here. Taking \( 2^s \)-th power of (8) and \( 2^{-s} \)-th power of (9), cancelling the term \( u^{2^{-k}} \), we get

\[ Au + Bu^{2^k} = 0, \tag{11} \]

where

\[
A = \left( \frac{b^{2^{s-2^k}}w^{2^k} + b^{2^{k-s}-2^k}w^{2^{k-s}}} {b^{2^{-s}+1-2^k-2^k}w^{2^{-s}+1} + b^{2^{-k-s}-2^{-k}}} \right)^{2^s}, \\
B = \left( \frac{bw)^{2^{-k-s}-2^k} + b^{2^{k-s}+1-2^k-2^k}w} {b^{2^{-s}+1-2^k-2^k}w^{2^{-s}+1} + b^{2^{-k-s}-2^{-k}}} \right)^{2^s}.
\]
Now we prove $A \neq 0$. Suppose $A = 0$, then

$$w^{2^k-2s}+2^k w^s = \left(\frac{b^{1-2^{-k+s}}+(bw)^{2^k+2^k}}{b^{2-s+2^k-2s}+b^{2^k+2^k-2s} w^{2^k-2s}+2^k} \right) \left(\frac{(bw)^{2^k-s+2^k-2s}+b^{2^k-s-2^k-2s}}{(bw)^{2^k}+b^{2^k+2^k}}\right).$$

Substituting $w$ with $\alpha^{2^k-1}$ and rearranging,

$$\alpha^{2^k-2s(2^k+3s+2^k-3)} = (RT^{-1})^{2^{2(k+s)-1}},$$

where

$$R = b^{2^2-s+2^k-2s}+b^{2^k+2^k-2s} w^{2^k-2s}+2^k,$$

$$T = (bw)^{2^k-s+2^k-2s}+b^{2^k-s-2^k-2s}.$$  

Notice that $3 \mid 2^{2(k+s)-1}$ and $3 \mid 2^{k+3s}+2^k-3$, which implies the left-hand side of (12) is not a cube, while the right-hand side is, which is a contradiction. It is easy to see that if $B = 0$, then by (11) the kernel $K = \{0\}$.

Now by (11) we obtain

$$u^{2^k} = A^{-2^k}B^{2^k+s} w^s,$$

$$u^{2^k-s} = B^{-2^k}A^{2-s} w^s.$$  

Substitute these two identities into $L_b(u) = 0$, then

$$Cu^{2^k} + Du^{2^k-s} = 0,$$

where $C = b + (bw)^{2^k} A^{-2^k} B^{2^k+s}$ and $D = b^{2^k-s} + (bw)^{2^k-2^k} B^{-2^k} A^{2-s}$. Next, we will show the coefficients $C, D$ will not be 0 at the same time. Otherwise,

$$Ab^{2^k-s} + (bw)^{2^k-2^k} B = 0,$$

$$Bb + (bw)^{2^k} A = 0.$$  

Combining the above two equations gives

$$Bb + (bw)^{2^k} b^{2^k-s-2^k-s} w^{2^k-s} B = 0.$$  

Cancelling $B$ in the above identity, replacing $w$ with $\alpha^{2^k-1}$ and rearranging, which yields

$$b^{(2^k+s-1)(1-2^k)} = \alpha^{(2^k-1)(2^k+1)}.$$  

Again, we see that the left-hand side is a 7-th power while the right-hand side is not, a contradiction. Finally, take the $2^{2s}$-th and $2^s$-th power on both sides of (11) and (13) respectively, then

$$A^{2^{2s}} u^{2^{2s}} + B^{2^{2s}} u^{2^{2s}+2s} = 0,$$

$$C^{2^s} u^{2^{2s}} + D^{2^s} u = 0.$$
Table 1
Known highly nonlinear differentially 4 uniform permutations.

<table>
<thead>
<tr>
<th>Function</th>
<th>Conditions</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(x^{2^i+1})</td>
<td>(n = 2k, k) odd, gcd((n, i) = 2)</td>
<td>[13]</td>
</tr>
<tr>
<td>(x^{2^i-2^i+1})</td>
<td>(n = 2k, k) odd, gcd((n, i) = 2)</td>
<td>[14]</td>
</tr>
<tr>
<td>(x^{-1})</td>
<td>(n) even</td>
<td>[1,16]</td>
</tr>
<tr>
<td>(x^{2^i+2^i+1})</td>
<td>(n = 4k, k) odd</td>
<td>[7,12]</td>
</tr>
<tr>
<td>(\alpha x^{2^i+1} + \alpha^2 x^{2^i-2^i+1})</td>
<td>Theorem 1.1</td>
<td>This article</td>
</tr>
</tbody>
</table>

Substitute \(u^{2^s}\) in (14) with \(C^{-2^s} D^{2^s} u\) we obtain

\[
A^{2^{2s}} C^{-2^s} D^{2^s} u + B^{2^{2s}} u^{2^{(k+t+2s+t)}} = 0. \tag{16}
\]

Notice it follows from 3 \(|k + s|\) that gcd\((k/t + 2s/t, 3k) = 1\) and by Lemma 4.1, we have \(L_b(u)\) has at most \(2^t\) solutions, i.e., \(|K| \leq 2^t\). The proof is completed. \(\square\)

5. Closing remarks and an open problem

We proved that, by choosing certain \(s\) and \(k\), the binomial function \(F(x) = \alpha x^{2^i+1} + \alpha^2 x^{2^i-2^i+2^i+s}\) defined on \(\mathbb{F}_{2^k}\) is a differentially 4 uniform permutation with high nonlinearity. This implies that \(F\) has the same resistance to both linear and differential attacks as the inverse function. It answers an open problem proposed in [7]. Now the list of all highly nonlinear permutations with differential uniformity 4 on fields with even degree is given in Table 1.

Some remarks on the CCZ-equivalence of the last function \(F\) in Table 1 to the known monomial functions are given below. It is proved in [8] that, when \(t = 1\) in Theorem 1.2, the function \(F\) is CCZ-inequivalent to the first and second functions. We expect the case of \(t = 2\) to be no different. For the inverse function, the Walsh spectrum is well known not to be a subset of \(\{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}\), while this is true for \(F\). So \(F\) is CCZ-inequivalent to the Inverse function. Clearly \(F\) is CCZ-inequivalent to the forth function as it exists in the fields with dimension \(4k\) with \(k\) odd.

The function \(F\) obtained in this paper is by changing certain conditions of a recently found quadratic APN functions. We surveyed the known quadratic APN functions listed in [6] and found just one other class that may have the same properties. Unfortunately, we cannot prove this result now and hence put it as an open problem.

Problem 5.1. Let \(s\) and \(k\) be positive integers with \(k + s\) divisible by three and gcd\((s, k) = t, gcd(3, s) = gcd(3, k) = 1, k/t\) is odd. Let \(u\) be a primitive element of \(\mathbb{F}_{2^{3k}}\) and let \(v, w \in \mathbb{F}_{2^k}\) with \(vw \neq 1\). Define the function \(G\) by

\[
G(x) = ux^{2^i+1} + u^{2k} x^{2^i-2^i+2^i+s} + vx^{2^i-2^i+1} + wu^{2k+1} x^{2^i+s}.
\]

Prove that \(F\) is a differentially \(2^t\) uniform permutation and the differential spectrum of \(F\) is \(\{0, 2^t\}\). Moreover, for any \(a, b \in \mathbb{F}_{2^3}\), \(|F^{W}(a, b)| \leq 2^{(n+t)/2}\) if \(n + t\) is even, and \(|F^{W}(a, b)| \leq 2^{((n+t)/(2))}\) if \(n + t\) is odd. Particularly, if \(t = 2\), \(F\) is a highly nonlinear differentially 4 uniform permutation over \(\mathbb{F}_{2^{3k}}\).

Acknowledgments

The authors would like to thank the anonymous referees for their invaluable comments and suggestions.
References