A Highly Nonlinear Differentially 4 Uniform Power Mapping That Permutes Fields of Even Degree

Carl Bracken[1], Gregor Leander[2]

[1]Department of Mathematics, National University of Ireland
Maynooth, Co. Kildare, Ireland

[2]Department of Mathematics, Technical University Denmark
Copenhagen, Denmark

January 13, 2009

Abstract

Functions with low differential uniformity can be used as the s-boxes of symmetric cryptosystems as they have good resistance to differential attacks. The AES (Advanced Encryption Standard) uses a differentially-4 uniform function called the inverse function. Any function used in a symmetric cryptosystem should be a permutation. Also, it is required that the function is highly nonlinear so that it is resistant to Matsui's linear attack. In this article we demonstrate that the highly nonlinear permutation $f(x) = x^{2^{2k}+2^k+1}$, discovered by Hans Dobbertin [7], has differential uniformity of four and hence, with respect to differential and linear cryptanalysis, is just as suitable for use in a symmetric cryptosystem as the inverse function.

1 Introduction

Functions with a low differential uniformity are interesting from the point of view of cryptography as they provide good resistance to differential attacks [11]. For a function to be used as an s-box of a symmetric cryptosystem it should be a permutation and defined on a field with even degree. It is also essential that the function has high nonlinearity so that it is resistant to Matsui's linear attack [10]. The lowest possible differential uniformity is 2 and functions with this property are called APN (almost perfect nonlinear). There has been much recent work and progress on APN functions (see [2],[3],[4],[5],[6]). However, at present there are no known APN permutations defined on fields of even degree and it is actually the most important open question in this field if such functions exist. This is why the AES (advanced encryption standard) uses a differentially 4 uniform function, namely the inverse function.

1

For the rest of the paper, let $L = \mathbb{F}_{2^n}$ for $n > 0$ and let L^* denote the set of non-zero elements of L. Let $\mathrm{Tr} : L \to \mathbb{F}_2$ denote the trace map from L to $\mathbb{F}_2$. For positive integers r, k by Tr_k^{rk} we denote the relative trace map from $\mathbb{F}_{2^{rk}}$ to $\mathbb{F}_{2^k}$ and by Tr^r the absolute trace from $\mathbb{F}_{2^r}$ to $\mathbb{F}_2$.

Definition 1 *A function $f : L \to L^*$ is said to be differentially δ uniform. if for any $a \in L^*, b \in L$, we have*

$$|\{x \in L : f(x + a) + f(x) = b\}| \leq \delta.$$

Definition 2 *Given a function $f : L \to L$, the **Fourier transform** of f is the function $\widehat{f} : L \times L^* \to \mathbb{Z}$ given by*

$$\widehat{f}(a, b) = \sum_{x \in L} (-1)^{\mathrm{Tr}(ax + bf(x))}.$$

The *Fourier spectrum* of f is the set of integers

$$\Lambda_f = \{\widehat{f}(a, b) : a, b \in L, b \neq 0\}.$$

The nonlinearity of a function f on a field $L = \mathbb{F}_{2^n}$ is defined as

$$NL(f) := 2^{n-1} - \frac{1}{2} \max_{x \in \Lambda_f} |x|.$$

The nonlinearity of a function measures its distance to the set of all affine maps on L. We thus call a function *maximally nonlinear* if its nonlinearity is as large as possible. If n is odd, its nonlinearity is upper-bounded by $2^{n-1} - 2^{\frac{n-1}{2}}$, while for n even a conjectured upper bound is $2^{n-1} - 2^{\frac{n}{2}-1}$. For odd n, we say that a function $f : L \longrightarrow L$ is *almost bent* (AB) when its Fourier spectrum is $\{0, \pm 2^{\frac{n+1}{2}}\}$, in which case it is clear from the upper bound that f is maximally nonlinear.

In an article of Hans Dobbertin [7] he offers a list of power mappings that permute fields of even degree and meet the conjectured nonlinearity bound of $2^{n-1} - 2^{\frac{n}{2}-1}$. Following Dobbertin's terminology we shall refer to such mapping as highly nonlinear permutations. In [7] Dobbertin conjectured that this list was complete and noted that this had been verified for $n \leq 22$. The inverse function (used in AES) is highly nonlinear and hence is on the list. One of the functions on Dobbertin's list is the power mapping $f(x) = x^{2^{2k}+2^k+1}$, defined on $\mathbb{F}_{2^{4k}}$, with k odd.

In this article we show that this function has differential uniformity of 4. We also provide another proof of this functions nonlinearity property. This means that this function has the same resistance to both the linear and differential attacks as the inverse function.

2 Differential Uniformity of $f(x) = x^{2^{2k}+2^k+1}$

As mentioned above there are no known permutations of even degree fields with differential uniformity of two. The following theorem shows that $x^{2^{2k}+2^k+1}$ has the next best (and best known) differential uniformity, which is four.

Theorem 1 *Let $f(x) = x^{2^{2k}+2^k+1}$ be defined on $\mathbb{F}_{2^{4k}}$. Then $f(x)$ has differential uniformity of four.*

Proof. We need to demonstrate that the equation

$$x^{2^{2k}+2^k+1} + (x+a)^{2^{2k}+2^k+1} = b$$

has no more than four solutions for all $a \in \mathbb{F}_{2^{4k}}^{*}$ and all $b \in \mathbb{F}_{2^{4k}}$.

Expansion of this expression yields

$$ax^{2^{2k}+2^k} + a^{2^k}x^{2^{2k}+1} + a^{2^{2k}}x^{2^k+1} + a^{2^k+1}x^{2^{2k}} + a^{2^{2k}+1}x^{2^k} + a^{2^{2k}+2^k}x + a^{2^{2k}+2^k+1} = b.$$

Next we replace x with xa and divide by $a^{2^{2k}+2^k+1}$ and obtain

$$x^{2^{2k}+2^k} + x^{2^{2k}+1} + x^{2^k+1} + x^{2^{2k}} + x^{2^k} + x + c \quad = \quad 0 \qquad (1)$$

where $c = a^{-2^{2k}-2^k-1}b + 1$.

Let Tr_k^{4k} denote the relative trace map from $\mathbb{F}_{2^{4k}}$ to $\mathbb{F}_{2^k}$.

As $\mathrm{Tr}_k^{4k}(x^{2^{2k}+2^k} + x^{2^{2k}+1} + x^{2^k+1} + x^{2^{2k}} + x^{2^k}) = 0$, Equation (1) implies $\mathrm{Tr}_k^{4k}(x+c) = 0$.

Which is equivalent to

$$x + x^{2^k} + x^{2^{2k}} + x^{2^{3k}} = t \qquad (2)$$

where $t = \mathrm{Tr}_k^{4k}(c)$. We note that $t \in \mathbb{F}_{2^k}$.

Equation (1) now becomes

$$x(x^{2^k} + x^{2^{2k}}) + x^{2^{2k}+2^k} + x^{2^{3k}} + t + c = 0.$$

Which implies

$$x(x + x^{2^{3k}} + t) + x^{2^{2k}+2^k} + x^{2^{3k}} + t + c = 0.$$

From which we obtain

$$x^2 + x^{2^{3k}+1} + xt + x^{2^{2k}+2^k} + x^{2^{3k}} + t + c \quad = \quad 0. \qquad (3)$$

We raise Equation (3) by 2^{2k} and get

$$x^{2^{2k+1}} + x^{2^k+2^{2k}} + x^{2^{2k}}t + x^{2^{3k}+1} + x^{2^k} + t + c^{2^{2k}} \quad = \quad 0. \qquad (4)$$

3

Now we add Equations (3) and (4) and make use of (2). This gives

$$(x + x^{2^{2k}})^2 + (t + 1)(x + x^{2^{2k}}) + c^{2^k} + c^{2^{3k}} \quad = \quad 0. \tag{5}$$

The remainder of the proof is divided into two cases. They are $t = 1$ and $t \neq 1$.
  If $t = 1$ then Equation (5) implies

$$x + x^{2^{2k}} = c^{2^{k-1}} + c^{2^{3k-1}}.$$

  We let $r = c^{2^{k-1}} + c^{2^{3k-1}}$. Therefore $x^{2^{2k}} = x + r$. Placing this into Equation (1) yields

$$(x + r)x^{2^k} + (x + r)x + x^{2^k+1} + x^{2^k} + c + r = 0.$$

Which we write as

$$x^2 + r(x + x^{2^k}) + x^{2^k} + r + c \quad = \quad 0. \tag{6}$$

Raising Equation (6) by 2^k we obtain

$$x^{2^{k+1}} + r^{2^k}(x^{2^k} + x + r) + x + r + r^{2^k} + c^{2^k} \quad = \quad 0. \tag{7}$$

Next we add Equations (6) and (7) to get

$$(x + x^{2^k})^2 + (r + r^{2^k} + 1)(x + x^{2^k}) + r^{2^k+1} + c + c^{2^k} + r^{2^k} \quad = \quad 0. \tag{8}$$

  Note that $r + r^{2^k} = x + x^{2^k} + x^{2^{2k}} + x^{2^{3k}} = t$, hence if $t = 1$ Equation (8) becomes

$$(x + x^{2^k})^2 + r^{2^k+1} + c + c^k + r^{2^k} = 0.$$

This implies $x + x^{2^k} = s$ where $s = \sqrt{r^{2^k+1} + c + c^k + r^{2^k}}$. Now we replace x^{2^k} by $x + s$ in Equation (6) and obtain

$$x^2 + x + rs + s + r + c = 0,$$

which can have no more than two solutions in x.
  Next we consider the case $t \neq 1$.
  We replace x with $(t + 1)z$ in Equation (5) and get

$$(t + 1)^2((z + z^{2^{2k}})^2 + (z + z^{2^{2k}})) + c^{2^k} + c^{2^{3k}} = 0.$$

Now let $y = z + z^{2^{2k}}$ so we have

$$(t + 1)^2(y^2 + y) + c^{2^k} + c^{2^{3k}} = 0.$$

This equation has at most two solutions in y. They are of the form $y = p$ and $y = p + 1$ for some fixed p. This implies that $z^{2^{2k}} = z + p$ or $z^{2^{2k}} = z + p + 1$. Note that $p \in \mathbb{F}_{2^{2k}}$.

4

If $z^{2^{2k}} = z + p$ then Equation (1) becomes

$$(t+1)^2((z+p)z^{2^k} + (z+p)z + z^{2^k+1}) + (t+1)(z^{2^k} + p) + c = 0,$$

which gives

$$(t+1)^2((z + z^{2^k})p + z^2) + (t+1)(z^{2^k} + p) + c \;=\; 0. \qquad (9)$$

We raise Equation (9) by 2^k and obtain

$$(t+1)^2((z + z^{2^k} + p)p^{2^k} + z^{2^{k+1}}) + (t+1)(z + p + p^{2^k}) + c^{2^k} \;=\; 0. \; (10)$$

Next we add Equations (9) and (10) to get

$$(t+1)^2((p+p^{2^k})(z+z^{2^k}) + (z+z^{2^k})^2 + p^{2^k+1}) + (t+1)(z+z^{2^k}+p^{2^k}) + c + c^{2^k} = 0,$$

which becomes

$$(t+1)^2(z + z^{2^k})^2 + ((t+1)^2(p + p^{2^k}) + (t+1))(z + z^{2^k})$$
$$+(t+1)^2 p^{2^k+1} + (t+1)p^{2^k} + c + c^{2^k} \;=\; 0. \quad (11)$$

Recall $t = x + x^{2^k} + x^{2^{2k}} + x^{2^{3k}} = (t+1)(z + z^{2^k} + z^{2^{2k}} + z^{2^{3k}})$.
Also $p + p^{2^k} = z + z^{2^k} + z^{2^{2k}} + z^{2^{3k}}$, hence $p + p^{2^k} = \frac{t}{t+1}$.
Therefore Equation (11) becomes

$$(t+1)^2((z + z^{2^k})^2 + (z + z^{2^k})) + (t+1)^2 p^{2^k+1}$$
$$+(t+1)p^{2^k} + c + c^{2^k} \;=\; 0. \qquad (12)$$

It can easily be verified that if we had assumed $z^{2^{2k}} = z + p + 1$ then the same computations as above would also yield Equation (12), so this case need not be considered.

Next we let $z + z^{2^k} = w$ and write Equation (12) as

$$(t+1)^2(w^2 + w) + (t+1)^2 p^{2^k+1} + (t+1)p^{2^k} + c + c^{2^k} = 0.$$

This equation has at most two solutions in w which take the form $w = q$ and $w = q + 1$ for some fixed q.

This implies that $z^{2^k} = z + q$ or $z^{2^k} = z + q + 1$.

If $z^{2^k} = z + q$ then $z^{2^{2k}} = z + q + q^{2^k}$ and Equation (1) becomes

$$(t+1)^2((z+q+q^{2^k})(z+q) + (z+q+q^{2^k})z + (z+q)z) + (t+1)(z+q^{2^k}) + c = 0.$$

This simplifies to

$$(t+1)^2 z^2 + (t+1)z + (t+1)^2(q^{2^k+1} + q^2) + (t+1)q^{2^k} + c = 0,$$

which is the same as

$$x^2 + x + (t+1)^2(q^{2^k+1} + q^2) + (t+1)q^{2^k} + c = 0.$$

If on the other hand $z^{2^k} = z + q + 1$, then we would obtain

$$x^2 + x + (t+1)^2(q^{2^k+1} + q^{2^k} + q^2 + q) + (t+1)(q+1)^{2^k} + c = 0.$$

Clearly, this pair of equations will allow no more than four solutions in x and the proof is complete. $\qquad\square$

Note that we did not need to assume that k is odd to derive the differential uniformity of four, however it is easy to see that the function is not a permutation if k is even as $g.c.d.(2^{4k} - 1, 2^{2k} + 2^k + 1) = 1$ if and only if k is odd.

3   Nonlinearity of $f(x) = x^{2^{2k}+2^k+1}$

In this section we give a slightly different proof of the fact that $x^{2^{2k}+2^k+1}$ has $\mathrm{NL}(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$. Most importantly, our proof also covers the case where the function is not a permutation, i.e., when k is even.

Technically, the main difference to Dobbertin's proof in [7] is that we are not going to use an $\mathbb{F}_{2^k}$ basis of $\mathbb{F}_{2^{4k}}$ to express elements in $\mathbb{F}_{2^{4k}}$ but rather a $\mathbb{F}_{2^{2k}}$ basis. This change makes some of the "lengthy but routine" computations, as Dobbertin states it, easier.

Theorem 2 *Let $f(x) = x^{2^{2k}+2^k+1}$ be defined on $\mathbb{F}_{2^{4k}}$. Then*

$$\mathrm{NL}(f) = 2^{n-1} - 2^{\frac{n}{2}-1}.$$

Proof. We have to show that for any non-zero b and any a the absolute value of the Fourier coefficient $\widehat{f}(a,b)$ is smaller or equal to 2^{2k+1}. There are two cases to consider. If k is odd, then f is a bijection and it is therefore enough to study the case $b = 1$. If k is even, then $\gcd(2^{2k} + 2^k + 1, 2^{4k} - 1) = 3$ and up to equivalence there are two different b to consider, namely the case $b = 1$ and b any non-cube. Here we remark that in the case k even we can always choose a non cube in $\mathbb{F}_{2^k}$ with out loss of generality. Thus, in both cases it is enough to study $b \in \mathbb{F}_{2^r}$. Moreover, we can restrict the case to elements $b \in \mathbb{F}_{2^k}$ such that $\mathrm{Tr}^k(b) = 1$.

Let γ be any non-zero element in $\mathbb{F}_{2^k}$ such that $\mathrm{Tr}^k(\gamma) = 1$. For simplicity we denote by $g_{\gamma^2}(x) = \mathrm{Tr}(\gamma^2 x^{2^{2k}+2^k+1})$ (we use γ^2 instead of γ to avoid dealing with square roots later on) . Furthermore, let $\alpha \in \mathbb{F}_{2^{2k}}$ be an element fulfilling the equation $\alpha^2 + \gamma\alpha + \gamma^3 = 0$. As $\mathrm{Tr}^k(\gamma) = 1$ the polynomial $\alpha^2 + \alpha + \gamma = 0$ is irreducible over $\mathbb{F}_{2^k}$ and by replacing α by $\alpha\gamma^{-1}$ and multiplying across by γ^2 we see that the polynomial $\alpha^2 + \gamma\alpha + \gamma^3 = 0$ is irreducible as well. Therefore $\alpha \notin \mathbb{F}_{2^k}$ and furthermore it holds that $\alpha^{2^k} + \alpha = \gamma$. Thus,

$$\mathrm{Tr}^{2k}(\alpha) = \mathrm{Tr}^k(\alpha^{2^k} + \alpha) = \mathrm{Tr}^k(\gamma) = 1.$$

6

This implies that the polynomial $x^2 + x + \alpha$ is irreducible over $\mathbb{F}_{2^{2k}}$ and finally every element in $\mathbb{F}_{2^{4k}}$ can be represented by $y + \omega a$, where $y, a \in \mathbb{F}_{2^{2k}}$ and $\omega \in \mathbb{F}_{2^{4k}}$ with $\omega^2 + \omega + \alpha = 0$. Using this expression for x we compute

$$
\begin{aligned}
g_{\gamma^2}(x) &= g_{\gamma^2}(y + \omega a) \\
&= \mathrm{Tr}(\gamma^2 (y + \omega a)^{2^{2k} + 2^k + 1}) \\
&= \mathrm{Tr}(\gamma^2 y^{2^{2k} + 2^k + 1}) \\
&\quad + \mathrm{Tr}(\gamma^2 (y^{2^{2k} + 2^k}(\omega a) + y^{2^{2k} + 1}(\omega a)^{2^k} + y^{2^k + 1}(\omega a)^{2^{2k}})) \\
&\quad + \mathrm{Tr}(\gamma^2 (y^{2^{2k}}(\omega a)^{2^k + 1} + y^{2^k}(\omega a)^{2^{2k} + 1} + y(\omega a)^{2^{2k} + 2^k})) \\
&\quad + \mathrm{Tr}(\gamma^2 (\omega a)^{2^{2k} + 2^k + 1}) \\
&= A + B + C + D.
\end{aligned}
$$

First we note that $A = 0$ as γ^2 and y are in $\mathbb{F}_{2^{2k}}$. Furthermore B can be simplified,

$$
\begin{aligned}
B &= \mathrm{Tr}(\gamma^2 y^{2^k + 1}(\omega a) + \gamma^2 y^2 (\omega a)^{2^k} + \gamma^2 y^{2^k + 1}(\omega a)^{2^{2k}}) \\
&= \mathrm{Tr}(\gamma^2 y^{2^k + 1}((\omega a) + (\omega a)^{2^{2k}}) + \gamma^2 y^2 (\omega a)^{2^k}) \\
&= \mathrm{Tr}(\gamma^2 y^2 (\omega a)^{2^k}).
\end{aligned}
$$

where the last equality follows as $\gamma^2 y^{2^k + 1}((\omega a) + (\omega a)^{2^{2k}})$ is in $\mathbb{F}_{2^{2k}}$. Now consider the term C. We first remark that $\gamma^2 y^{2^k}(\omega a)^{2^{2k} + 1}$ is in the subfield $\mathbb{F}_{2^{2k}}$ and thus

$$
\begin{aligned}
C &= + \mathrm{Tr}(\gamma^2 (y^{2^{2k}}(\omega a)^{2^k + 1} + y(\omega a)^{2^{2k} + 2^k})) \\
&= \mathrm{Tr}(\gamma^2 y((\omega a)^{2^k + 1} + (\omega a)^{2^{2k} + 2^k})).
\end{aligned}
$$

Therefore

$$
\begin{aligned}
g(x) &= g(y + \omega a) \\
&= \mathrm{Tr}(y\left(\gamma(\omega a)^{2^{k-1}} + \gamma^2 (\omega a)^{2^k + 1} + \gamma^2 (\omega a)^{2^{2k} + 2^k}\right) + \gamma^2 (\omega a)^{2^{2k} + 2^k + 1}).
\end{aligned}
$$

The important observation is that this expression is linear in y. Thus, the function belongs to the generalized Maiorana McFarland type of functions. Next, we compute an expression of g using the absolute trace on $\mathbb{F}_{2^{2k}}$ denoted by Tr^{2k}. For this we make use of the following equations

$$
\omega + \omega^{2^{2k}} = 1
$$

and

$$
\omega^{2^{2k} + 2^k + 1} + (\omega^{2^{2k} + 2^k + 1})^{2^{2k}} = \alpha
$$

that follow from the fact that the two solutions of

$$
x^2 + x + \alpha = 0
$$

are ω and $\omega^{2^{2k}}$.

$$
\begin{aligned}
g(y + \omega a) &= \operatorname{Tr}^{2k}\left(y\left(\gamma a^{2^{k-1}}(\omega + \omega^{2^{2k}})^{2^{k-1}} + \gamma^2(a(\omega + \omega^{2^{2k}}))^{2^k+1}\right)\right) \\
&\quad + \operatorname{Tr}^{2k}\left(\gamma^2 a^{2^{2k}+2^k+1}(\omega^{2^{2k}+2^k+1} + (\omega^{2^{2k}+2^k+1})^{2^{2k}})\right) \\
&= \operatorname{Tr}^{2k}\left(y\left(\gamma a^{2^{k-1}} + \gamma^2 a^{2^k+1}\right) + \alpha\gamma^2 a^{2^k+2}\right).
\end{aligned}
$$

From now on the proof continues very much like Dobbertin's original proof. We denote by $\mu(y) = (-1)^{\operatorname{Tr}^{2k}(y)}$ and

$$
\pi(a) = \gamma a^{2^{k-1}} + \gamma^2 a^{2^k+1}.
$$

We compute

$$
\begin{aligned}
\widehat{g}(u + \omega v) &= \sum_{y,a \in \mathbb{F}_{2^{2k}}} \mu(y\pi(a) + \alpha\gamma^2 a^{2^k+2} + uy + va) \\
&= \sum_a \mu(\alpha\gamma^2 a^{2^k+2} + va) \sum_y \mu(y(\pi(a) + u)) \\
&= 2^{2k} \sum_{a,\pi(a)=u} \mu(\alpha\gamma^2 a^{2^k+2} + va).
\end{aligned}
$$

For any u we have to study the set $M = \{a \mid \pi(a) = u\}$ and in particular its possible size. First note that

$$
\pi(a) = \pi(a + c)
$$

implies

$$
\begin{aligned}
0 &= \pi(a) + \pi(a + c) + (\pi(a) + \pi(a + c))^{2^k} \\
&= \gamma(c^{2^{k-1}} + c^{2^{2k-1}}) \\
&= \gamma(c + c^{2^k})^{2^{k-1}}
\end{aligned}
$$

and we conclude $c \in \mathbb{F}_{2^k}$. Therefore, we can equivalently study the set

$$
\{c^2 \in \mathbb{F}_{2^k} \mid \pi(a_0 + c^2) = u\}
$$

where a_0 is an element in M. Note that we use c^2 instead of c to get rid of the power 2^{k-1}. Considering the equation

$$
\pi(a_0) + \pi(a_0 + c^2) = 0
$$

we get the following equation for c

$$
c^4 + (a_0^{2^k} + a_0)c^2 + \gamma^{-1}c = 0 \tag{13}
$$

which immediately implies $|M| \in \{0, 1, 2, 4\}$. As $\widehat{(g)}(u + \omega v) \le 2^{2k}|M|$ the only case we need to care about for proving the theorem is the case $|M| = 4$. In this case the set M consists of elements

$$
M = \{a_0, a_0 + c_0, a_0 + c_1, a_0 + c_0 + c_1\}
$$

where c_0, c_1 are solutions of (13) and thus $c_0 c_1 (c_0 + c_1) = \gamma^{-1}$. Next we compute

$$
\begin{aligned}
\sum_{a \in M} \mathrm{Tr}^{2k}(\alpha \gamma^2 a^{2^k + 2} + va) &= \mathrm{Tr}^{2k}(\alpha \gamma^2 (a_0^{2^k + 2} + (a_0 + c_0)^{2^k + 2} \\
&\quad + (a_0 + c_1)^{2^k + 2} + (a_0 + c_0 + c_1)^{2^k + 2})) \\
&= \mathrm{Tr}^{2k}(\alpha \gamma^2 (c_0 c_1^2 + c_1 c_0^2)) \\
&= \mathrm{Tr}^{2k}(\alpha \gamma^2 (c_0 c_1 (c_0 + c_1))) \\
&= \mathrm{Tr}^{2k}(\alpha \gamma) \\
&= \mathrm{Tr}^{k}(\gamma(\alpha + \alpha^{2^k})) \\
&= \mathrm{Tr}^{k}(\gamma^2) = 1
\end{aligned}
$$

which implies

$$
\widehat{g}(u + \omega v) = \sum_{a \in M} \mu(\alpha a^{2^k + 2} + va) = \pm 2^{2k+1}.
$$

$\square$

4   Closing Remarks and Open Problems

We have demonstrated that the function $f(x) = x^{2^{2k} + 2^k + 1}$ has the same resistance to both differential and linear attacks as the inverse function. The fact that it can permute the field when k is odd means it could be used in a cryptosystem acting on 12 bits. We now list all the known highly nonlinear permutations with differential uniformity of 4. For power mappings we conjecture this list to be complete.

f(x)	Conditions	Ref.
$x^{2^s + 1}$	$n = 2k, \ k$ odd $gcd(n, s) = 2$	[8]
$x^{2^{2s} - 2^s + 1}$	$n = 2k, \ k$ odd $gcd(n, s) = 2$	[9]
x^{-1}	n even	[1]
$x^{2^{2k} + 2^k + 1}$	$n = 4k, \ k$ odd	This article

Open Problem 1 *Find more highly nonlinear permutations of even degree fields with differential uniformity of 4.*

Open Problem 2 *Find a function, defined on a field of even degree, with higher nonlinearity than $2^{n-1} - 2^{\frac{n}{2}-1}$ or prove that such a function can't exist.*

References

[1] Thomas Beth, Cunsheng Ding, "On almost perfect nonlinear permutations", *EUROCRYPT*, (1993), 65–76.

[2] C. Bracken, E. Byrne, N. Markin, G. McGuire, "New families of quadratic almost perfect nonlinear trinomials and multinomials", *Finite Fields and Their Applications*, Vol. 14, Issue 3, July 2008, 703–714.

[3] C. Bracken, E. Byrne, N. Markin, G. McGuire, "A few more quadratic APN functions", *Cryptography and Communications*, to appear.

[4] L. Budaghyan, C. Carlet, G. Leander, "Constructing new APN functions from known ones", *Finite Fields and Their Applications*, to appear.

[5] L. Budaghyan, C. Carlet, P. Felke, and G. Leander, "An infinite class of quadratic APN functions which are not equivalent to power mappings", *Proceedings of ISIT 2006*, Seattle, USA, July 2006.

[6] L. Budaghyan, C. Carlet, G. Leander, "Another class of quadratic APN binomials over F_{2^n}: the case n divisible by 4," *Proceedings of WCC 07*, pp. 49–58, Versaille, France, April 2007.

[7] H. Dobbertin, "One-to-one highly nonlinear power functions on GF(2^n)", *Appl. Algebra Eng. Commun. Comput*, **9**, (1998), 139-152.

[8] R. Gold, Maximal recursive sequences with 3 valued cross-correlation functions, *IEEE Trans.inform.theory*, **14**, (1968), 154-156.

[9] T. Kasami, Weight distributions of B-C-H codes, *Combinatorial Mathematics and applications.* **ch. 20** (1969)

[10] M. Matsui, Linear Cryptanalysis Method for DES Cipher, EURO-CRYPT93, LNCS 765, pp.386-397, Springer-Verlag, 1994.

[11] K. Nyberg, "Differentially uniform mappings for cryptography", *Advances in Cryptology-EUROCRYPT 93, Lecture Notes in Computer Science*, Springer-Verlag, pp. 55-64, 1994.