The Walsh Spectrum of a New Family of APN Functions *

Yue Zhou† and Chao Li‡

Department of Mathematics and System Sciences,
National University of Defence Technology,
Changsha 410073, Hunan , China
†*E-mail: gabelozhou@gmail.com,*
‡*E-mail: lichao_nudt@sina.com*

Abstract: The extended Walsh spectrum of a new family of APN functions is computed out. It turns out that the walsh spectrum of these functions are the same as that of Gold functions.

Keywords: almost perfect nonlinear; extended Walsh spectrum; nonlinearity; quadratic function

1. Introduction and Preliminaries

The differential cryptanalysis presented by Biham and Shamir[2] is based on the study of how differences in an input can affect the resultant differences at the output. The resistance to differential attacks for a function f from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$, used as an S-box in the cipher, is high when the value

$$\delta_f = \max_{a,b\in\mathbb{F}_{2^n},a\neq 0} |\{x \in \mathbb{F}_{2^n} : f(x+a) + f(x) = b\}|,$$

is small. The functions with the smallest possible differential uniformity[3] , that is, with smallest δ_f, oppose an optimum resistance to the differential attack. They are called almost perfect nonlinear(APN).

The *extended walsh transform* of f at (a, b) is given by

$$f^W(a,b) = \sum_{x\in\mathbb{F}_{2^n}} \chi(ax + bf(x)),$$

*This work was supported by the Natural Science Foundation of China(60573028) and the open research fund of National Mobile Communications Research Laboratory, Southeast University(W200825).

where $\chi(x) = (-1)^{Tr(x)}$, for each $a, b \in \mathbb{F}_{2^n}$. Then we can define the extended walsh spectrum of f as the set

$$\Lambda_f = \{f^W(a,b) : a, b \in \mathbb{F}_{2^n}, b \neq 0\},$$

The linear cryptanalysis introduced by Matsui[4] is based on finding affine approximations to the action of a cipher. And the *nonlinearity* of a function is the value

$$NL(f) = 2^{n-1} - \frac{1}{2} \max_{a,b \in \mathbb{F}_{2^n}, b \neq 0} |f^W(a,b)|,$$

which equals the minimum Hamming distance between all nonzero linear combinations of the coordinate functions of f and all affine Boolean functions on n variables. It has been proved[5] that $NL(f) \geq 2^{n-1} - 2^{\frac{n-1}{2}}$, and the functions achieving the maximal possible nonlinearity $NL(f) = 2^{n-1} - 2^{\frac{n-1}{2}}$ possess the best resistance to the linear attack, which are called almost bent(AB) or maximum nonlinear. Furthermore, it is showed that $f(x)$ is AB if and only if it has a 3-valued extended walsh spectrum $\{0, \pm 2^{\frac{n+1}{2}}\}$, in which case n must be odd[6].

CCZ equivalence[6] is a standard measure to determine whether two functions are essentially the same for AB and APN properties, because δ_f and Λ_f is invariant under it. This relation generalizes *extended affine*(EA) equivalence. A family of APN functions is new if they are CCZ inequivalent to any previously know family.

All known APN functions are only in a short list of power functions, which are all contained in Table 1, and all known AB functions are contained in Table 2, until 2006 when new examples began to appear in the literature. The first function was given in[7]. Until now, there are 8 families of new quadratic APN functions, which are all presented in Table 3. They have been shown CCZ-inequivalent to any power APN functions on $\mathbb{F}_{2^n}$, for some n, by technical construction and calculating the CCZ-invariants, like extended walsh spectrum[6] or Γ-rank[7]. However, it has not been proved that these functions are CCZ-inequivalent to all power functions on $\mathbb{F}_{2^n}$, for any n, or for infinite n.

By calculating the extended walsh spectrum of APN functions, we can get some important results. Firstly and apparently, the nonlinearity of these functions. Secondly, by comparing the extended walsh spectrum, we may tell whether a new APN function is CCZ-inequivalent to those known APN functions for infinite n.

It is well known that every AB function on $\mathbb{F}_{2^n}$ is also APN function[5]. If n is odd, f is quadratic and f is APN also, then it is necessarily AB[6].

Table 1. Known APN Power Functions on $\mathbb{F}_{2^n}$

functions	exponents	conditions
Gold[3]	2^i+1	$gcd(i,n)=1$
Kasami[12]	$2^{2i}-2^i+1$	$gcd(i,n)=1$
Welch[14]	2^t+3	$n=2t+1$
Niho[13]	$2^t+2^{\frac{t}{2}-1}$, t even; $2^t+2^{\frac{3t+1}{2}-1}$, t odd	$n=2t+1$
Inverse[3]	$2^{2t}-1$	$n=2t+1$
Dobbertin[15]	$2^{4t}+2^{3t}+2^{2t}+2^t-1$	$n=5t$

Table 2. Known AB Power Functions on $\mathbb{F}_{2^n}$,where n is odd

functions	exponents	conditions
Gold[3]	2^i+1	$gcd(i,n)=1$
Kasami[12]	$2^{2i}-2^i+1$	$gcd(i,n)=1$
Welch[21]	2^t+3	$n=2t+1$
Niho[21]	$2^t+2^{\frac{t}{2}-1}$, t even; $2^t+2^{\frac{3t+1}{2}-1}$, t odd	$n=2t+1$

Table 3. Known APN quadratic Functions on $\mathbb{F}_{2^n}$

No.	functions	conditions	Walsh spectrum
1[16]	$x^{2^s+1}+wx^{2^{ik}+2^{mk+s}}$	$n=3k$,$gcd(k,3)=gcd(s,3k)=1$, $k\geq 4, i=sk \bmod 3, m=3-i$, $ord(w)=2^{2k}+2^k+1$	unknown
2[17]	$x^{2^s+1}+wx^{2^{ik}+2^{mk+s}}$	$n=4k$,$gcd(k,2)=gcd(s,2k)=1$, $k\geq 3, i=sk \bmod 4, m=4-i$, $ord(w)=2^{3k}+2^{2k}+2^k+1$	unknown
3[1]	$x^{2^{2s}+2^i}+bx^{q+1}$ $+cx^{q(2^{2i}+2^i)}$	$n=2m$,$m\geq 3$,$q=2^m, c^{q+1}=1$ $c\notin\{\lambda^{(2^i+1)(q-1)},\lambda\in\mathbb{F}_{2^n}\}$ $gcd(i,m)=1$,$cb^q+b\neq 0$	5 values, proved in Theorem 1 of the present paper
4[1]	$x(x^{2^i}+x^q+cx^{2^iq})$ $+x^{2^i}(c^qx^q+sx^{2^iq})+x^{(2^i+1)q}$	$n=2m$,$m\geq 3$,$q=2^m, gcd(i,m)=1$, $s\notin\{\mathbb{F}_q\}, x^{2^i+1}+cx^{2^i}+c^qx+1$ is irreducible over $\mathbb{F}_{2^n}$	unknown
5[18]	$x^3+tr(x^9)$	$n\geq 7$,$n>2p$, for the smallest possible $p>1$, such that $p\neq 3, gcd(p,n)=1$	5 values, n even; 3 values, n odd[10]
6[19]	$u^{2^k}x^{2^{-k}+2^{k+s}}+ux^{2^s+1}$ $+vx^{2^{-k}+1}+wu^{2^k+1}x^{2^{k+s}+2^s}$	$3\mid(k+s),(s,3k)=(3,k)=1$, $n=3k$,u is primitive in $\mathbb{F}_{2^{3k}}$, $v,w\in\mathbb{F}_{2^k}$,$v\neq w^{-1}$	unknown
7[20]	$\alpha x^{2^s+1}+\alpha^{2^k}x^{2^{k+s}+2^k}$ $+\beta x^{2^k+1}+\sum_{i=1}^{k-1}\gamma_i x^{2^{k+1}+2^i}$	$gcd(k,s)=1, 2\nmid k, 2\nmid s$, α,β is primitive in $\mathbb{F}_{2^{2k}}$, , $\gamma_i\in\mathbb{F}_{2^{2k}}$,$v\neq w^{-1}$	5 values[9]
8[20]	$ux^{2^{-k}+2^{k+s}}+u^{2^k}x^{2^s+1}$ $+vx^{2^{k+s}+2^s}$	$3\mid(k+s),(s,3k)=1$, $n=3k,\ 3\nmid k$, u,v is primitive in $\mathbb{F}_{2^k}$	unknown

When n is even, an APN function may have a large extended walsh spectrum (more than 5 values), which means it could be less resistant to linear attack. It should be remarked that not all quadratic APN functions always have 5 values, which is the same as the Gold functions for even n. The extended walsh spectrum of a quadratic APN function may have more than 5 values, and an example with 7-valued spectrum was shown in[8]. Because all the new APN functions in Table 3 are quadratic, we only to calculate the extended walsh spectrum when n is even, and that of two functions(No. 5 and No. 7) in Table 3 has been worked out.

The new family of APN trinomial (No.3) was given in [1], along with No.4. And it was shown to be CCZ inequivalent to Dobbertin functions for any m, and inequivalent to any APN power functions when $m = 3$.

In this paper, we compute the extended walsh spectrum of these trinomials, and show that it is 5-valued, which is the same as that of the Gold functions x^{2^i+1}, where $(i, n) = 1$. Furthermore, we know that these new functions can't be proved to be CCZ-inequivalent to Gold functions by calculating the extended walsh spectrum.

To prove the main result of this paper, we need the following two lemmas.

Lemma 1.1. *Let $d = gcd(m, n)$, then $gcd(2^m - 1, 2^n - 1) = 2^d - 1$ and*

$$gcd(2^m - 1, 2^n + 1) = \begin{cases} 1 + 2^d & \text{if } m/d \text{ is even and } n/d \text{ is odd} \\ 1 & \text{otherwise.} \end{cases} \tag{1}$$

Lemma 1.2. [9] *Let n, s, d be integers, and $gcd(n, s) = 1$. Then linearized polynomial*

$$\mathcal{L}(x) = \sum_{i=0}^{d} a_i x^{2^{is}} \in \mathbb{F}_{2^n}[x],$$

has at most 2^d roots in $\mathbb{F}_{2^n}$.

2. The extended walsh Spectrum of New APN Functions

Let m, i be integers, where $m \geq 3$, and let $n = 2m$. In [1] a new quadratic function was shown to be APN over $\mathbb{F}_{2^n}$:

$$f(x) = x^{2^{2i}+2^i} + \beta x^{q+1} + \theta x^{q(2^{2i}+2^i)} \tag{2}$$

where $q = 2^m, \theta \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^{2m}}\}, \theta^{q+1} = 1, gcd(i, m) = 1, \theta\beta^q + \beta \neq 0$.

From lemma 1.1, we know that $gcd(2^{2m}-1, 2^i+1) = 1$ when i is even, since $gcd(i, m) = 1$. Then x^{2^i+1} is a permutation on $\mathbb{F}_{2^{2m}}$, which means there is no θ such that $\theta \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^{2m}}\}$ and $\theta^{q+1} = 1$. Hence, we can let i be odd directly.

Since $\mathbb{F}_{2^{2m}}$ has even degree, the extended walsh spectrum of f is not determined even though it is APN.

Theorem 2.1. *Let $f(x)$ be defined on $L = \mathbb{F}_{2^{2m}}$ as in (2), i is odd, and let $f^W(a,b)$ be the extended walsh spectrum of $f(x)$. Then*

$$\Lambda_f = \{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n+2}{2}}\}$$

Proof. By definition, we have

$$\begin{aligned} f^W(a,b)^2 &= \sum_{x,\ u \in L} \chi(ax + bf(x) + a(x+u) + bf(x+u)) \\ &= \sum_{x,\ u \in L} \chi(au + b(f(u) + x^{2^{2i}}u^{2^i} + \beta x^q u + \theta x^{q2^{2i}} u^{q2^i} \\ &\quad + u^{2^{2i}}x^{2^i} + \beta x u^q + \theta u^{q2^{2i}} x^{q2^i})) \\ &= \sum_{u \in L} \chi(au + bf(u)) \sum_{x \in L} \chi(x\mathcal{L}_b(u)), \end{aligned}$$

where $\chi(x) = (-1)^{Tr(x)}, x \in \mathbb{F}_{2^{2m}}$ and

$$\begin{aligned} \mathcal{L}_b(u) &= su^{2^i} + s^{2^{-i}}u^{2^{-i}} + b\beta u^{2^m} + (b\beta)^{2^m}u^{2^m} \\ &= su^{2^i} + s^{2^{-i}}u^{2^{-i}} + tu^{2^m}, \end{aligned}$$

for $s = (b + (b\theta)^{2^m})^{2^{-i}}$, $t = b\beta + (b\beta)^{2^m}$.

Furthermore, let U_b be the kernel of $\mathcal{L}_b(u)$, then we have

$$f^W(a,b)^2 = 2^n \sum_{u \in U_b} \chi(au + bf(u)),$$

It is easy to verified that $\phi(x) = Tr(ax + bf(x))$ is linear on U_b, which is a linear subspace of $\mathbb{F}_{2^{2m}}$, Thus $\chi(\phi(\cdot))$ is a character of U_b, from which we deduce that

$$|f^W(a,b)| = \begin{cases} 2^m|U_b|^{1/2} & \text{if } \phi(au + bf(u)) = 0, \forall u \in U_b, \\ 0 & otherwise. \end{cases} \tag{3}$$

Since U_b is a linear subspace and n is even , we get that $|U_b|$ must be an even power of 2 to keep sure that $|f^W(a,b)|$ is an integer. Now, what remains to be calculated is $|U_b|$.

First, assume that $s = 0$, then we have $b = (b\theta)^{2^m}, \mathcal{L}_b(u) = tu^{2^m}$. If $t = 0$, then we have $\theta = \beta^{2^m-1}$, which means $\theta\beta^{2^m} + \beta = \beta^{2^{2m}-1} + \beta = 0$. It contradicts the condition of θ and β, hence $t \neq 0$, from which we can deduce that $\mathcal{L}_b(u) = tu^{2^m}$ has only one root.

Second, suppose $t = 0$, then $\mathcal{L}_b(u) = su^{2^i} + s^{2^{-i}}u^{2^{-i}}$. Due to $gcd(i, 2m) = 1$ and lemma1.2, it has at most 2^2 roots.

Now, we assume that both s and t are non-zero.For an nonzero $u \in U_b$, let's consider

$$u\mathcal{L}_b(u) = su^{2^i+1} + s^{2^{-i}}u^{2^{-i}+1} + tu^{2^m+1} = 0,$$

Since $t = b\beta + (b\beta)^{2^m}$, $tu^{2^m+1} \in \mathbb{F}_{2^m}$, which means $su^{2^i+1} + s^{2^{-i}}u^{2^{-i}+1} \in \mathbb{F}_{2^m}$. Thus we have

$$(su^{2^i+1} + s^{2^m}u^{2^{m+i}+2^m})^{2^{-i}} = su^{2^i+1} + s^{2^m}u^{2^{m+i}+2^m},$$

Then $g(u) \triangleq su^{2^i+1} + s^{2^m}u^{2^{m+i}+2^m} \in \mathbb{F}_{2^i}$. Furthermore, as $gcd(i, m) = 1$ and $g(u) \in \mathbb{F}_{2^m}$, we have $g(u) \in \mathbb{F}_2$.

If $g(u) = 0$, then $su^{2^i+1} = (su^{2^i+1})^{2^m}$, i.e. $su^{2^i+1} \in \mathbb{F}_{2^m}$. According to $s = (b + (b\theta)^{2^m})^{2^{-i}}$, we have

$$(b^{2^m} + b\theta)^{2^{-i}}(u^{2^i+1})^{2^m} = (b + (b\theta)^{2^m})^{2^{-i}}(u^{2^i+1}),$$

which means

$$\frac{b + (b\theta)^{2^m}}{b^{2^m} + b\theta} = (u^{2^i+1})^{(2^m-1)2^i},$$

which is equal to

$$\frac{\theta b + b^{2^m}}{\theta(b^{2^m} + b\theta)} = \frac{1}{\theta} = (u^{2^i+1})^{(2^m-1)2^i}, \tag{4}$$

since $\theta^{2^m+1} = 1$. Because (4) contradicts the condition of $f(x)$, we have $g(u) + 1 = 0$.

Now, we use a trick to get a new linearized equation. Let $\Delta_i(x, y) = xy^{2^i} + x^{2^i}y$, $\phi(x) = (x^{2^{\tau k}+1})^{2^{-\gamma k}}$. And it can be verified that

$$(x + y)(y\phi(x) + x\phi(y)) + xy\phi(x + y) = \Delta_{\tau-\gamma}(x, y)\Delta_\gamma^{2^{-\gamma k}}(x, y),$$

The, we choose some nonzero $v \in U_b$ and $v \neq u$, let $\phi(u) = g(u)$, and consider

$$(u + v)(v(g(u) + 1) + u(g(v) + 1)) + uv(g(u + v) + 1) = 0,$$

which equals to

$$s^{2^m}(\Delta_{i+m}(u, v) + \Delta_{-m}^{2^m}) + u^2 + v^2 + uv = 0,$$

$$s^{2^m}(u^{2^{i+m}}v+v^{2^{i+m}}u)(u^{2^m}v+v^{2^m}u)+u^2+v^2+uv=0, \qquad (5)$$

Replace u by vw in (5) and divide it by v^2 to obtain

$$s^{2^m}v^{2^{m+i}+2^m}(w+w^{2^{m+i}})(w+w^{2^m})+w^2+w+1=0, \qquad (6)$$

If $w+w^{2^m}=0$, i.e. $w\in\mathbb{F}_{2^m}$, then $w^2+w+1=0$, which means $w\in\mathbb{F}_{2^2}\backslash\mathbb{F}_2$ and $2|m$.

If $w+w^{2^m}\neq 0$, raising (6) to the 2^m-th power and adding it to (6), we get

$$(w+w^{2^m})(sv^{2^i+1}(w^{2^m}+w^{2^i})+s^{2^m}v^{2^{m+i}+2^m}(w^{2^{m+i}}+w)+(w+w^{2^m})+1)=0,$$

which divided by $w+w^{2^m}$ is

$$sv^{2^i+1}(w^{2^m}+w^{2^i})+s^{2^m}v^{2^{m+i}+2^m}(w^{2^{m+i}}+w)+(w+w^{2^m})+1=0,$$

Due to v obeys the expression $g(v)+1=sv^{2^i+1}+s^{2^m}v^{2^{m+i}+2^m}+1=0$, the equation above becomes

$$sv^{2^i+1}(w+w^{2^i})+s^{2^m}v^{2^{m+i}+2^m}(w^{2^{m+i}}+w^{2^m})+1=0, \qquad (7)$$

Now, consider our original equation $\mathcal{L}_b(u)$, and replace u with vw, we have

$$\mathcal{L}_b(vw)=sv^{2^i}w^{2^i}+s^{2^{-i}}v^{2^{-i}}w^{2^{-i}}+tv^{2^m}w^{2^m},$$

Then we have

$$\begin{aligned} w^{2^m} &= t^{-1}(sv^{2^i-2^m}w^{2^i}+s^{2^{-i}}v^{2^{-i}-2^m}w^{2^{-i}}),\\ w^{2^{m+i}} &= t^{-2^i}(s^{2^i}v^{2^{2i}-2^{m+i}}w^{2^{2i}}+sv^{1-2^{m+i}}w), \end{aligned}$$

After substituting the expression of w^{2^m} and $w^{2^{m+i}}$ into (7) and then raising to 2^i-th power, we obtain an equation of this form

$$\delta_3w^{2^{3i}}+\delta_2w^{2^{2i}}+\delta_1w^{2^i}+\delta_0w+1=0,$$

which has at most 2^3 roots, since $gcd(i,2m)=1$, due to lemma 1.2.

From all the discussion above, we know that $|U_b|$ is at most $2+2^3=10$. Furthermore, as $|U_b|$ must be an even power of 2, it follows that $|U_b|\leq 4$. Since there is no AB functions on $\mathbb{F}_2^{2m}$, the extended walsh spectrum of $f(x)$ is $\{0,\pm2^{\frac{n}{2}},\pm2^{\frac{n+2}{2}}\}$

□

In fact, we've attempted to use the method above on the other functions in Table 3, but it doesn't work well. And we present some open problems.

Open problem 1: Calculate the extended walsh spectrum of all the new APN quadric functions in Table 3.

Open problem 2: Construct new APN quadric functions on $\mathbb{F}_{2^n}$, with extended walsh spectrum more than 5, when n is even.

References

[1]. L. Budaghyan and C. Carlet,*Classes of Quadratic APN Trinomials and Hexanomials and Related Structures* (Preprint, 2007).

[2]. E. Biham and A. Shamir,*Differential Cryptanalysis of DES-like Cryptosystems.* Journal of cryptology, vol.4, No.1, pp.3-72, 1991 .

[3]. K. Nyberg,*Differentially uniform mappings for cryptography.* Advances in Cryptography, *EUROCRYPT'93*, Lecture Notes in Computer Science, Springer-Verlag, New York, 765, pp.55-64, 1994. .

[4]. M. Matsui,*Linear cryptanalysis method for DES cipher.* Advances in Cryptology, *EUROCRYPT'93*,Lecture Notes in Computer Science, Springer-Verlag, pp.386-397, 1994

[5]. F. Chabaud and S. Vaudenay, *Links between differential and linear cryptanalysis.* Advances in Cryptography, *EUROCRYPT'94*, Lecture Notes in Computer Science, Springer-Verlag, New York, 950, pp.356-365, 1995.

[6]. A. Carlet, P. Charpin and V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems.* Designs, Codes and Cryptography 15(2), 125-156,1998.

[7]. Y. Edel, G. Kyureghyan, A. Pott, *A new APN function which is not equivalent to a power mapping.* IEEE Transactions on Information Theory 52(2), 744-747, 2006

[8]. J. Dillion, *APN Polynomials and Related Codes.* Polynomials over Finite Fields and Applications, Banff International Research Station, Nov. 2006

[9]. C. Bracken, E. Byrne, N. Markin and G. McGuire, *Determining the Nonlinearity of New Family of APN Functions.* AAECC 2007, Lecture Notes in Computer Science, Springer-Verlag, New York, 4851, pp. 72-79, 2007

[10]. C. Bracken, E. Byrne, N. Markin and G. McGuire, *On the Walsh Spectrum of a New APN Function.* Cryptography and Coding 2007, Lecture Notes in Computer Science, Springer-Verlag, New York, 4887, pp. 92-98, 2007

[11]. H. Dobbertin, *Another Proof of Kasami's Theorem.* Designs, Codes and Cryptography, Vol.17, pp.177-180, 1999

[12]. T. Kasami, *The weight enumberators for several classes of subcodes of the second order binary Reed-Muller codes.* Inform. and Control, 18, pp.180-194, 1993

[13]. H. Dobbertin, *Almost perfct nonlinear power fucntions over $GF(2^n)$: the Niho case.* Inform. and Comput., 151, pp. 57-72, 1999

[14]. H. Dobbertin, *Almost perfct nonlinear power fucntions over $GF(2^n)$: the Welch case.* IEEE Trans. Inform. Theory, 45, pp. 1271-1275, 1999

[15]. H. Dobbertin, *Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5.* D. Jungnickel and H. Niederreiter ed. Proceddings of

Finite Fields and Applications FQ5, Augsberg, Germany, Springer, pp.113-121, 2000

[16]. L. Budaghyan, C. Carlet, P. Felke, G. Leander. *An infinite class of quadratic APN functions which are not equivalent to power mappings.* Proceedings of the IEEE International Symposium on Information Theory 2006, Seattle, USA, Jul. 2006.

[17]. L. Budaghyan, C. Carlet, P. Felke, G. Leander. *Another class of quadratic APN binomials over* $\mathbb{F}_{\not\geq\ltimes}$ *: the case n divisible by 4.* Proceedings of the International Workshop on Coding and Cryptograhy, WCC 2007, dedicated to the memory of Hans Dobbertin, pp. 49-58, Versailles,France, Apr. 2007.

[18]. L. Budaghyan, C. Carlet, P. Felke, G. Leander.*Construction new APN functions from known ones.* Finite Fields and Applications(Preprint submitted)

[19]. C. Bracken, E. Byrne, N. Markin and G. McGuire, *An Infinite Family of Quadratic Quarinomial APN Functions.* (preprint,2007)

[20]. C. Bracken, E. Byrne, N. Markin and G. McGuire, *New Families of Quadratic Almost Perfect Nonlinear Trinomials and Multinomials.*(preprint,2007)

[21]. H. Hollmann and Q. Xiang, *A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences.*Finite Fields and Its Applications 7, pp. 253-286, 2001