Some Results on the Known Classes of Quadratic APN Functions

Lilya Budaghyan, Tor Helleseth, Nian Li(✉), and Bo Sun

Department of Informatics, University of Bergen,
Postboks 7803, 5020 Bergen, Norway
{Lilya.Budaghyan,Tor.Helleseth,Nian.Li,Bo.Sun}@uib.no

Abstract. In this paper, we determine the Walsh spectra of three classes of quadratic APN functions and we prove that the class of quadratic trinomial APN functions constructed by Göloğlu is affine equivalent to Gold functions.

Keywords: APN function · Quadratic function · Walsh spectrum

1 Introduction

For given positive integers n and m, a function F from the finite field $\mathbb{F}_{2^n}$ to the finite field $\mathbb{F}_{2^m}$ is called a vectorial Boolean function or an (n, m)-function, and in the case when $m = 1$ it is simply called a Boolean function. When $m = n$ an (n, n)-function has a unique representation as a univariate polynomial over $\mathbb{F}_{2^n}$ of the form

$$F(x) = \sum_{i=0}^{2^n-1} a_i x^i, \qquad a_i \in \mathbb{F}_{2^n}.$$

Boolean and vectorial Boolean functions have many applications in mathematics and information theory. In particular, they play an important role in cryptography.

In modern society, exchange and storage of information in an efficient, reliable and secure manner is of fundamental importance. Cryptographic primitives are used to protect information against eavesdropping, unauthorized changes and other misuse. In the case of symmetric cryptography ciphers are designed by appropriate composition of nonlinear Boolean functions. For example, the security of block ciphers depends on S-boxes which are (n, m)-functions. For most of cryptographic attacks on block ciphers there are certain properties of functions which measure the resistance of the S-box to these attacks. The differential attack introduced by Biham and Shamir is one of the most efficient cryptanalysis tools for block ciphers [2]. It is based on the study of how differences in an input can affect the resulting difference at the output. An (n, m)-function F is called differentially δ-uniform if the equation $F(x + a) - F(x) = b$ has at most δ

This work was supported by the Norwegian Research Council.

S. El Hajji et al. (Eds.): C2SI 2017, LNCS 10194, pp. 3–16, 2017.
DOI: 10.1007/978-3-319-55589-8_1

solutions for every nonzero element a of $\mathbb{F}_{2^n}$ and every b in $\mathbb{F}_{2^m}$. Functions with the smallest possible differential uniformity contribute an optimal resistance to the differential attack [34]. In this sense differentially 2^{n-m}-uniform functions, called perfect nonlinear (PN), are optimal. However, PN functions exist only for n even and $m \leq n/2$ [35]. An important case are differentially 2-uniform functions with $n = m$, called almost perfect nonlinear (APN), which have the smallest possible differential uniformity.

Another powerful attack on block ciphers is linear cryptanalysis by Matsui which is based on finding affine approximations to the action of a cipher [33]. The nonlinearity $NL(F)$ of an (n, m)-function F is the minimum Hamming distance between all the component functions of F (that is, the functions $\mathrm{tr}_1^m(vF(x))$ where

$$\mathrm{tr}_1^m(x) = x + x^2 + \cdots + x^{2^{m-1}}$$

denotes the absolute trace function of $\mathbb{F}_{2^m}$ and v is any nonzero element of $\mathbb{F}_{2^m}$) and all affine Boolean functions over $\mathbb{F}_{2^n}$. The nonlinearity quantifies the level of resistance of the function to the linear attack: the higher is the nonlinearity $NL(F)$ the better is the resistance of F [21]. The functions achieving the upper bound on nonlinearity are called bent functions. All bent functions are also PN and vice versa, that is, these functions have optimal resistance against both linear and differential attacks. As mentioned above, PN (or bent) functions do not exist when $m = n$. In this case, when also n is odd, functions with the best possible nonlinearity are called almost bent (AB). When n is even the upper bound on nonlinearity is still to be determined. All AB functions are APN, but the converse is not true in general. However, for n odd all quadratic APN functions are also AB.

The nonlinearity $NL(F)$ of an (n, m) function F can be expressed by means of the Walsh transform. The Walsh transform of F at $(\alpha, \beta) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ is defined by

$$W_F(\alpha, \beta) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_1^m(\beta F(x)) + \mathrm{tr}_1^n(\alpha x)},$$

and the Walsh spectrum of F is the set

$$\{W_F(\alpha, \beta) : \alpha \in \mathbb{F}_{2^n}, \beta \in \mathbb{F}_{2^m}^*\}.$$

Then

$$NL(F) = 2^{n-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}_{2^n}, \beta \in \mathbb{F}_{2^m}^*} |W_F(\alpha, \beta)|.$$

The Walsh spectrum of AB functions consists of three values $0, \pm 2^{\frac{n+1}{2}}$. The Walsh spectrum of a bent function is $\{\pm 2^{\frac{n}{2}}\}$.

There are several equivalence relations of functions for which differential uniformity and nonlinearity are invariant. Due to these equivalence relations, having only one APN (respectively, AB) function, one can generate a huge class of APN (respectively, AB) functions.

Two functions F and F' from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ are called

- affine equivalent (or linear equivalent) if $F' = A_1 \circ F \circ A_2$, where the mappings A_1 and A_2 are affine (resp. linear) permutations of $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^n}$, respectively;
- extended affine equivalent (EA-equivalent) if $F' = A_1 \circ F \circ A_2 + A$, where the mappings $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, $A_1 : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, $A_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are affine, and where A_1, A_2 are permutations;
- Carlet-Charpin-Zinoviev equivalent (CCZ-equivalent) if for some affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ the image of the graph of F is the graph of F', that is, $\mathcal{L}(G_F) = G_{F'}$ where $G_F = \{(x, F(x)) \mid x \in \mathbb{F}_{2^n}\}$ and $G_{F'} = \{(x, F'(x)) \mid x \in \mathbb{F}_{2^n}\}$.

Although different, these equivalence relations are connected to each other. It is obvious that linear equivalence is a particular case of affine equivalence, and that affine equivalence is a particular case of EA-equivalence. As shown in [20], EA-equivalence is a particular case of CCZ-equivalence and every permutation is CCZ-equivalent to its inverse. The algebraic degree of a function (if it is not affine) is invariant under EA-equivalence but, in general, it is not preserved by CCZ-equivalence.

There are six known infinite families of power APN functions. They are presented in Table 1. There are also eleven known infinite families of quadratic APN polynomilas CCZ-inequivalent to power functions. They are given in Table 2. Families 3, 4 and 11 in Table 2 are proven to be a part of a general binary construction of APN functions [18].

Classification of APN functions is complete for $n \leq 5$ [9]: for these values of n the only APN functions, up to CCZ-equivalence, are power APN functions, and up to EA-equivalence, are power APN functions and those APN functions constructed in [16]. For $n = 6$ classification is complete for quadratic APN functions: 13 quadratic APN functions are found in [10] and, as proven in [26], up to CCZ-equivalence, these are the only quadratic APN functions. The only known APN function CCZ-inequivalent to power functions and to quadratic functions was found in [9,27] for $n = 6$. For $n = 7$ and $n = 8$, as shown in a recent work [37], there are, respectively, more than 470 and more than a thousand

Table 1. Known APN power functions x^d on $\mathbb{F}_{2^n}$.

Functions	Exponents d	Conditions	$d^\circ(x^d)$	Proven
Gold	$2^i + 1$	$\gcd(i, n) = 1$	2	[28,34]
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$	$i + 1$	[31,32]
Welch	$2^t + 3$	$n = 2t + 1$	3	[23]
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$	$(t + 2)/2$ $t + 1$	[22]
Inverse	$2^{2t} - 1$	$n = 2t + 1$	$n - 1$	[1,34]
Dobbertin	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$n = 5i$	$i + 3$	[24]

Table 2. Known classes of quadratic APN polynomials CCZ-inequivalent to power functions on $\mathbb{F}_{2^n}$.

N°	Functions	Conditions	References
1–2	$x^{2^s+1}+\alpha^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n=pk$, $\gcd(k,p)=\gcd(s,pk)=1$, $p\in\{3,4\}$, $i=sk \bmod p$, $m=p-i$, $n\geq 12$, α primitive in $\mathbb{F}_{2^n}^*$	[13]
3	$x^{2^{2i}+2^i}+bx^{q+1}+cx^{q(2^{2i}+2^i)}$	$q=2^m$, $n=2m$, $\gcd(i,m)=1$, $\gcd(2^i+1,q+1)\neq 1$, $cb^q+b\neq 0$, $c\notin\{\lambda^{(2^i+1)(q-1)},\lambda\in\mathbb{F}_{2^n}\}$, $c^{q+1}=1$	[12]
4	$x(x^{2^i}+x^q+cx^{2^iq})$ $+x^{2^i}(c^qx^q+sx^{2^iq})+x^{(2^i+1)q}$	$q=2^m$, $n=2m$, $\gcd(i,m)=1$, $c\in\mathbb{F}_{2^n}$, $s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q$, $X^{2^i+1}+cX^{2^i}+c^qX+1$ is irreducible over $\mathbb{F}_{2^n}$	[12]
5	$x^3+a^{-1}\mathrm{tr}_1^n(a^3x^9)$	$a\neq 0$	[14,15]
6	$x^3+a^{-1}\mathrm{tr}_3^n(a^3x^9+a^6x^{18})$	$3\|n$, $a\neq 0$	[14]
7	$x^3+a^{-1}\mathrm{tr}_3^n(a^6x^{18}+a^{12}x^{36})$	$3\|n$, $a\neq 0$	[14]
8–10	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}$ $+vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n=3k$, $\gcd(k,3)=\gcd(s,3k)=1$, $v,w\in\mathbb{F}_{2^k}$, $vw\neq 1$, $3\|(k+s)$, u primitive in $\mathbb{F}_{2^n}^*$	[3]
11	$\alpha x^{2^s+1}+\alpha^{2^k}x^{2^{k+s}+2^k}$ $+\beta x^{2^k+1}+\sum_{i=1}^{k-1}\gamma_i x^{2^{k+i}+2^i}$	$n=2k$, $\gcd(s,k)=1$, s,k odd, $\beta\notin\mathbb{F}_{2^k}$, $\gamma_i\in\mathbb{F}_{2^k}$, α not a cube	[3,4]

CCZ-inequivalent quadratic APN functions. For n odd all power APN functions and the known APN binomials are permutations (see [13,19]). For n even the only known APN permutation is constructed in [11] for $n=6$. Existence of APN permutations for even $n\geq 8$ is an open problem.

A class of APN functions over $\mathbb{F}_{2^n}$

$$x^3+\mathrm{tr}_1^n(x^9)$$

was constructed by Budaghyan, Carlet and Leander in [14]. Later, they generalized this result in [15] to the APN function $F_0(x)$ of the form

$$F_0(x)=x^3+a^{-1}\mathrm{tr}_1^n(a^3x^9) \tag{1}$$

for any positive integer n and any nonzero element a in $\mathbb{F}_{2^n}$, and they also obtained two other classes of APN functions over $\mathbb{F}_{2^n}$

$$F_1(x)=x^3+a^{-1}\mathrm{tr}_3^n(a^3x^9+a^6x^{18}) \tag{2}$$
$$F_2(x)=x^3+a^{-1}\mathrm{tr}_3^n(a^6x^{18}+a^{12}x^{36}) \tag{3}$$

for any positive integer n divisible by 3 and any nonzero element a in $\mathbb{F}_{2^n}$ and where $\mathrm{tr}_3^n(x)=\sum_{i=0}^{n/3-1}x^{2^{3i}}$ is the trace function from $\mathbb{F}_{2^n}$ to its subfield $\mathbb{F}_{2^3}$. When n is even each of the functions F_0, F_1 and F_2 defines two CCZ-inequivalent

functions one for $a = 1$ and one for any $a \neq 1$, that is, all together they give six different functions. When n is odd each of the functions F_0, F_1 and F_2 defines only one function, up to CCZ-inequivalence, that is, all together they give three different functions [15]. In Table 2 the functions F_0, F_1 and F_2 correspond to families 5, 6 and 7, respectively. In the present paper we determine the Walsh spectra of the functions F_0, F_1 and F_2. The Walsh spectra of the remaining functions in Tables 1 and 2 have been determined in [6–8,17,28,30,36]. Note that the Walsh spectrum of the function F_0 with $a = 1$ was previously found in [5] and we generalize this result to any $a \neq 0$. The results on the Walsh spectra show that all the known families of quadratic APN functions have Gold like Walsh spectra. Note that there exists a quadratic APN function for $n = 6$ with Walsh spectrum different from Gold [10].

In 2015 a family of quadratic APN trinomials on $\mathbb{F}_{2^n}$

$$G(x) = x^{2^k+1} + \left(\mathrm{tr}_m^n(x)\right)^{2^k+1}, \tag{4}$$

with $\gcd(k, n) = 1$ and $n = 2m = 4t$, was constructed in [29]. It was claimed there to be CCZ-inequivalent to power functions. However, in the present paper we prove that this family is in fact affine equivalent to Gold power functions.

2 Walsh Spectra of F_1 and F_2

In this section, we determine the Walsh spectra of the APN functions F_1 and F_2. According to the definition, for any $b, c \in \mathbb{F}_{2^n}$, one gets

$$\begin{aligned} g_i(x) = \mathrm{tr}_1^n(bF_i(x) + cx) &= \mathrm{tr}_1^n(bx^3 + ba^{-1}\mathrm{tr}_3^n(a^3x^9 + a^6x^{18})^i + cx) \\ &= \mathrm{tr}_1^n(bx^3 + cx) + \mathrm{tr}_1^n(ba^{-1}\mathrm{tr}_3^n(a^3x^9 + a^6x^{18})^i) \\ &= \mathrm{tr}_1^n(bx^3 + cx) + \mathrm{tr}_1^3\mathrm{tr}_3^n(ba^{-1}\mathrm{tr}_3^n(a^3x^9 + a^6x^{18})^i) \\ &= \mathrm{tr}_1^n(bx^3 + cx) + \mathrm{tr}_1^3\mathrm{tr}_3^n(\mathrm{tr}_3^n(ba^{-1})(a^3x^9 + a^6x^{18})^i) \\ &= \mathrm{tr}_1^n(bx^3 + cx + \mathrm{tr}_3^n(ba^{-1})(a^3x^9 + a^6x^{18})^i) \end{aligned}$$

for $i \in \{1, 2\}$. For simplicity, denote $\mathrm{tr}_3^n(ba^{-1}) = \delta^2$. By a direct calculation, one obtains that

$$\begin{aligned} &g_i(x) + g_i(x+u) + g_i(u) \\ &= \mathrm{tr}_1^n(bx^2u + bxu^2 + \delta^2(a^3x^8u + a^3xu^8 + a^6x^2u^{16} + a^6x^{16}u^2)^i) \\ &= \mathrm{tr}_1^n\big(x((bu)^{2^{-1}} + bu^2 + (\delta^{2/i}a^3u)^{2^{-3}} + \delta^{2/i}a^3u^8 + \delta^{1/i}a^3u^8 + (\delta^{1/i}a^3u)^{2^{-3}})\big) \\ &= \mathrm{tr}_1^n\big(x((\delta^{2/i} + \delta^{1/i})a^3u^8 + bu^2 + (bu)^{2^{-1}} + ((\delta^{2/i} + \delta^{1/i})a^3u)^{2^{-3}})\big), \end{aligned} \tag{5}$$

which implies that

$$\begin{aligned} |W_{F_i}(b, c)|^2 &= \sum_{x\in\mathbb{F}_{2^n}} \sum_{u\in\mathbb{F}_{2^n}} (-1)^{g_i(x)+g_i(x+u)} \\ &= \sum_{u\in\mathbb{F}_{2^n}} (-1)^{g_i(u)} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_1^n(xL^i_{a,b,\delta}(u))}, \end{aligned}$$

where $L^i_{a,b,\delta}(u)$ is defined as

$$L^i_{a,b,\delta}(u) = (\delta^{2/i} + \delta^{1/i})a^3u^8 + bu^2 + (bu)^{2^{-1}} + ((\delta^{2/i} + \delta^{1/i})a^3u)^{2^{-3}}. \quad (6)$$

Note that $g_i(u) + g_i(u+v) + g_i(v) = \mathrm{tr}_1^n(vL^i_{a,b,\delta}(u))$ due to (5) and (6). This means that for any u satisfying $L^i_{a,b,\delta}(u) = 0$ and any $v \in \mathbb{F}_{2^n}$ we have

$$g_i(u+v) = g_i(u) + g_i(v)$$

which implies that

$$|W_{F_i}(b,c)|^2 = 0, \qquad \text{or} \qquad 2^n \cdot |\{x \in \mathbb{F}_{2^n} : L^i_{a,b,\delta}(u) = 0\}|. \quad (7)$$

In what follows, we discuss the number of solutions $u \in \mathbb{F}_{2^n}$ to $L^i_{a,b,\delta}(u) = 0$ by adopting Dobbertin's method [25], which also was used by Bracken et al. in [5] to determine the Walsh spectrum of $F_0(x)$ for the case of $a = 1$.

For simplicity, define $\theta_i = (\delta^{2/i} + \delta^{1/i})a^3$ for $i = 1, 2$. Then $L^i_{a,b,\delta}(u) = 0$ can be written as $\theta_i u^8 + bu^2 + (bu)^{2^{-1}} + (\theta_i u)^{2^{-3}} = 0$ and it can be readily verified that

$$uL^i_{a,b,\delta}(u) = \phi_i(u) + \phi_i(u)^{2^{-1}},$$

where $\phi_i(u)$ is given as

$$\phi_i(u) = bu^3 + \theta_i u^9 + \theta_i^{\frac{1}{2}} u^{\frac{9}{2}} + \theta_i^{\frac{1}{4}} u^{\frac{9}{4}}. \quad (8)$$

Then, if $L^i_{a,b,\delta}(u) = 0$, we must have $\phi_i(u) \in \mathbb{F}_2$.

Proposition 1. *Let $a, b \in \mathbb{F}_{2^n}$ with $ab \neq 0$ and $\delta^2 = \mathrm{tr}_3^n(ba^{-1})$. If $\delta^{2/i} + \delta^{1/i} \neq 0$, then $L^i_{a,b,\delta}(u) = 0$ if and only if $\phi_i(u) = 0$ for $i = 1, 2$.*

Proof. If $\phi_i(u) = 0$, we have $L^i_{a,b,\delta}(u) = 0$; and if $L^i_{a,b,\delta}(u) = 0$, we have $\phi_i(u) \in \mathbb{F}_2$. Thus, to complete the proof, we need to show that $L^i_{a,b,\delta}(u) = 0$ implies that $\phi_i(u) = 0$ for $i = 1, 2$. Suppose that $\phi_i(u) = 1$, one then gets $b = \theta_i u^6 + \theta_i^{1/2} u^{3/2} + \theta_i^{1/4} u^{-3/4} + u^{-3}$ which together with $\theta_i = (\delta^{2/i} + \delta^{1/i})a^3$ leads to

$$\frac{b}{a} = (\delta^{\frac{2}{i}} + \delta^{\frac{1}{i}})a^2u^6 + (\delta^{\frac{2}{i}} + \delta^{\frac{1}{i}})^{\frac{1}{2}} a^{\frac{1}{2}} u^{\frac{3}{2}} + (\delta^{\frac{2}{i}} + \delta^{\frac{1}{i}})^{\frac{1}{4}} a^{-\frac{1}{4}} u^{-\frac{3}{4}} + a^{-1}u^{-3}. \quad (9)$$

For convenience, define $\mathrm{tr}_3^n(a^2u^6) = t$ and $\mathrm{tr}_3^n(a^{-1}u^{-3}) = r$. Notice that $\delta^{\frac{1}{2}} = \delta^4$ and $\delta^{\frac{1}{4}} = \delta^2$ since $\delta \in \mathbb{F}_{2^3}$. Then by $\mathrm{tr}_3^n(ba^{-1}) = \delta^2$ and (9) one has that

$$\delta^2 = \mathrm{tr}_3^n(\frac{b}{a}) = (\delta^{\frac{2}{i}} + \delta^{\frac{1}{i}})t + (\delta^{\frac{1}{i}} + \delta^{\frac{1}{2i}})t^{\frac{1}{4}} + (\delta^{\frac{1}{2i}} + \delta^{\frac{1}{4i}})r^{\frac{1}{4}} + r. \quad (10)$$

Rewrite (10) with respect to the variable r we have

$$(\delta^{\frac{1}{2i}} + \delta^{\frac{1}{4i}})r^2 + r + (\delta^{\frac{2}{i}} + \delta^{\frac{1}{i}})t + (\delta^{\frac{1}{i}} + \delta^{\frac{1}{2i}})t^2 + \delta^2 = 0.$$

Note that $\delta^{\frac{1}{2i}} + \delta^{\frac{1}{4i}} \neq 0$ due to $\delta^{\frac{2}{i}} + \delta^{\frac{1}{i}} \neq 0$. Then the above equation has solution $r \in \mathbb{F}_{2^3}$ if and only if

$$\mathrm{tr}_1^3((\delta^{\frac{1}{2i}} + \delta^{\frac{1}{4i}})((\delta^{\frac{2}{i}} + \delta^{\frac{1}{i}})t + (\delta^{\frac{1}{i}} + \delta^{\frac{1}{2i}})t^2 + \delta^2)) = 0. \tag{11}$$

It can be readily verified that for $i = 1, 2$ we have

$$(\delta^{\frac{1}{2i}} + \delta^{\frac{1}{4i}})^2(\delta^{\frac{2}{i}} + \delta^{\frac{1}{i}})^2 = (\delta^{\frac{1}{2i}} + \delta^{\frac{1}{4i}})(\delta^{\frac{1}{i}} + \delta^{\frac{1}{2i}}),$$

which implies that (11) holds if and only if

$$\mathrm{tr}_1^3((\delta^{\frac{1}{2i}} + \delta^{\frac{1}{4i}})\delta^2) = 0.$$

Observe that $(\delta^{\frac{1}{2i}} + \delta^{\frac{1}{4i}})\delta^2 = (\delta^4 + \delta^2)\delta^2 = \delta^6 + \delta^4$ if $i = 1$, and it equals $(\delta^2+\delta)\delta^2 = \delta^4+\delta^3$ if $i = 2$. Thus, no matter which case we arrive at $\mathrm{tr}_1^3(\delta^3+\delta) = 0$. By $\mathrm{tr}_1^3(\delta^3) = \mathrm{tr}_1^3(\delta)$ and $\delta^7 = 1$ we have $\delta^3 + \delta^6 + \delta^5 = \delta + \delta^2 + \delta^4$ which leads to $\delta = 0, 1$, a contradiction with $\delta^{2/i}+\delta^{1/i} \neq 0$. Therefore, if $\delta^{2/i}+\delta^{1/i} \neq 0$, then there is no solution $r \in \mathbb{F}_{2^3}$ to (10) and $L^i_{a,b,\delta}(u) = 0$ if and only if $\phi_i(u) = 0$. This completes the proof.

Proposition 2. *Let $a, b \in \mathbb{F}_{2^n}$ with $ab \neq 0$ and $\delta^2 = \mathrm{tr}_3^n(ba^{-1})$. Then $L^i_{a,b,\delta}(u) = 0$ defined by (6) has at most four roots in $\mathbb{F}_{2^n}$ for any $i \in \{1, 2\}$.*

Proof. If $\theta_i = 0$, i.e., $\delta^{2/i} + \delta^{1/i} = 0$, then (6) is reduced to $bu^2 + (bu)^{2^{-1}} = 0$ which has at most four roots in $\mathbb{F}_{2^n}$ for any nonzero b. Next we consider the case $\theta_i \neq 0$. By Proposition 1, for this case we have $L^i_{a,b,\delta}(u) = 0$ if and only if $\phi_i(u) = 0$. Thus, to complete the proof, it suffices to show that $\phi_i(u) = 0$ has at most four roots in $\mathbb{F}_{2^n}$ for any $i \in \{1, 2\}$. If $\phi_i(u) = 0$ has no nonzero solution for some θ_i and b, then the desired result follows. Now let v be any fixed nonzero solution of $\phi_i(u) = 0$, then for any u satisfying $\phi_i(u) = 0$ we have

$$u(u + v)\phi_i(v) + v(u + v)\phi_i(u) + uv\phi_i(u + v) = 0.$$

A direct calculation based on (8) gives

$$\theta_i^{\frac{1}{2}}(u^2v^{\frac{9}{2}} + v^2u^{\frac{9}{2}} + u^5v^{\frac{3}{2}} + v^5u^{\frac{3}{2}}) = \theta_i^{\frac{1}{4}}(u^2v^{\frac{9}{4}} + v^2u^{\frac{9}{4}} + u^3v^{\frac{5}{4}} + v^3u^{\frac{5}{4}}),$$

which can be written as

$$\theta_i^{\frac{1}{4}}(u^4v + uv^4)(u^{\frac{1}{2}}v + uv^{\frac{1}{2}}) = (u^2v + uv^2)(u^{\frac{1}{4}}v + uv^{\frac{1}{4}}) \tag{12}$$

since $\theta_i \neq 0$. Then, let $u = vz$, one obtains that

$$\theta_i^{\frac{1}{4}}v^{\frac{9}{4}}(z^4 + z)(z^{\frac{1}{2}} + z) = (z^2 + z)(z^{\frac{1}{4}} + z). \tag{13}$$

Note that v is a fixed nonzero element which means that z is uniquely determined by u. Thus, one can conclude that the number of solutions $z \in \mathbb{F}_{2^n}$ to (13) is no less than that of $u \in \mathbb{F}_{2^n}$ to $\phi_i(u) = 0$. Let $w = z^2 + z$ and rewrite (13) as

$$w\Omega_i(w) := \theta_i^{\frac{1}{4}}v^{\frac{9}{4}}(w^2 + w)w^{\frac{1}{2}} + w(w^{\frac{1}{2}} + w^{\frac{1}{4}}) = 0. \tag{14}$$

Observe that (12) holds for any u satisfying $\phi_i(u) = 0$ and the solution set of $\phi_i(u) = 0$ is an $\mathbb{F}_2$-linear space due to Proposition 1. Then, one can conclude that the solution sets of both (13) and (14) are $\mathbb{F}_2$-linear spaces. Assume that w_1, w_2 and $w_1 + w_2$ are solutions of (14), then we have

$$0 = \Omega_i(w_1) + \Omega_i(w_2) + \Omega_i(w_1 + w_2) = \theta_i^{\frac{1}{4}} v^{\frac{9}{4}} (w_1^{\frac{1}{2}} w_2 + w_2^{\frac{1}{2}} w_1)$$

since (14) holds if and only if $\Omega_i(w) = 0$, which leads to $w_1 w_2^2 + w_2^2 w_1 = w_1 w_2 (w_1 + w_2) = 0$, i.e., $w_1 = 0$, $w_2 = 0$ or $w_1 = w_2$. This means that (14) has at most two distinct solutions in $\mathbb{F}_{2^n}$ and then (13) has at most four solutions in z since $w = z^2 + z$. This completes the proof.

Theorem 1. *The Walsh spectra of both functions F_1 and F_2 defined by (2) and (3) respectively are $\{0, \pm 2^{(n+1)/2}\}$ if n is odd and $\{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}$ otherwise.*

Proof. The Walsh transform of F_i, $i = 1, 2$, takes values from $\{0, \pm 2^{(n+1)/2}\}$ if n is odd and takes values from $\{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}$ if n is even. This follows from (7) and Proposition 2.

The Walsh transform takes all three values for n odd and all 5 values for n even since quadratic functions are plateaud and there exists no bent function from $\mathbb{F}_{2^n}$ to itself, while in case of n even quadratic APN functions have some bent components.

3 Walsh Spectrum of F_0

Bracken et al. in [5] had determined the Walsh spectrum of the APN function F_0 for the case of $a = 1$. In this section, we determine its Walsh spectrum for any nonzero element $a \in \mathbb{F}_{2^n}$ by using the same techniques. By the definition, for any $b, c \in \mathbb{F}_{2^n}$, one gets

$$\begin{aligned} \mathrm{tr}_1^n(bF_0(x) + cx) &= \mathrm{tr}_1^n(bx^3 + ba^{-1}\mathrm{tr}_1^n(a^3x^9) + cx) \\ &= \mathrm{tr}_1^n(bx^3 + cx + \mathrm{tr}_1^n(ba^{-1})a^3x^9). \end{aligned}$$

For simplicity, let $\mathrm{tr}_1^n(ba^{-1}) = \delta$ and $g_0(x) = \mathrm{tr}_1^n(bF_0(x) + cx)$. Then, by a direct calculation, one obtains that

$$\begin{aligned} & g_0(x) + g_0(x+u) + g_0(u) \\ &= \mathrm{tr}_1^n(bx^2u + bxu^2 + \delta a^3x^8u + \delta a^3xu^8) \\ &= \mathrm{tr}_1^n\big(x((bu)^{2^{-1}} + bu^2 + (\delta a^3u)^{2^{-3}} + \delta a^3u^8)\big), \end{aligned} \tag{15}$$

which implies that

$$\begin{aligned} |W_{F_0}(b,c)|^2 &= \sum_{x\in\mathbb{F}_{2^n}} \sum_{u\in\mathbb{F}_{2^n}} (-1)^{g_0(x)+g_0(x+u)} \\ &= \sum_{u\in\mathbb{F}_{2^n}} (-1)^{g_0(u)} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_0^n(xL^0_{a,b,\delta}(u))}, \end{aligned}$$

where $L^0_{a,b,\delta}(u)$ is defined as

$$L^0_{a,b,\delta}(u) = (bu)^{2^{-1}} + bu^2 + (\delta a^3 u)^{2^{-3}} + \delta a^3 u^8. \tag{16}$$

Note that $g_0(u) + g_0(u+v) + g_0(v) = \mathrm{tr}_1^n(vL^0_{a,b,\delta}(u))$ due to (15) and (16). This means that for any u satisfying $L^0_{a,b,\delta}(u) = 0$ and any $v \in \mathbb{F}_{2^n}$ we have

$$g_0(u+v) = g_0(u) + g_0(v)$$

which implies that

$$|W_{F_0}(b,c)|^2 = 0, \text{ or } 2^n | \{x \in \mathbb{F}_{2^n} : L^0_{a,b,\delta}(u) = 0\}|. \tag{17}$$

Next we aim to determine the number of solutions to $L^0_{a,b,\delta}(u) = 0$ in order to determine the possible values of the Walsh spectrum of $F_0(x)$. First, if $\delta = \mathrm{tr}_1^n(ba^{-1}) = 0$, then $L^0_{a,b,\delta}(u) = 0$ is reduced to $L^0_{a,b,0}(u) = (bu)^{2^{-1}} + bu^2 = 0$ which has at most 4 roots in $\mathbb{F}_{2^n}$. Now we assume that $\delta = \mathrm{tr}_1^n(ba^{-1}) = 1$, then $L^0_{a,b,\delta}(u) = 0$ is reduced to $L^0_{a,b,1}(u) = (bu)^{2^{-1}} + bu^2 + (a^3u)^{2^{-3}} + a^3u^8 = 0$, and it is straightforward to verify that

$$uL^0_{a,b,1}(u) = \phi_0(u) + \phi_0(u)^{2^{-1}}, \tag{18}$$

where $\phi_0(u)$ is defined by

$$\phi_0(u) = bu^3 + a^3u^9 + a^{\frac{3}{2}}u^{\frac{9}{2}} + a^{\frac{3}{4}}u^{\frac{9}{4}}.$$

Proposition 3. *Let $a, b \in \mathbb{F}_{2^n}$ with $\delta = \mathrm{tr}_1^n(ba^{-1}) = 1$. Then $L^0_{a,b,1}(u) = 0$ if and only if $\phi_0(u) = 0$.*

Proof. According to (18), we have $L^0_{a,b,1}(u) = 0$ if $\phi_0(u) = 0$; and $\phi_0(u) \in \mathbb{F}_2$ if $L^0_{a,b,1}(u) = 0$. Thus, to complete the proof, we need to show that $L^0_{a,b,1}(u) = 0$ implies that $\phi_0(u) = 0$. Suppose that $\phi_0(u) = 1$, one then gets $b = a^3u^6 + a^{3/2}u^{3/2} + a^{3/4}u^{-3/4} + u^{-3}$ which leads to

$$ba^{-1} = a^2u^6 + a^{\frac{1}{2}}u^{\frac{3}{2}} + a^{-\frac{1}{4}}u^{-\frac{3}{4}} + a^{-1}u^{-3}.$$

This contradicts with the condition that $\mathrm{tr}_1^n(ba^{-1}) = 1$. This completes the proof.

Proposition 4. *Let $a, b \in \mathbb{F}_{2^n}$ with $ab \neq 0$ and $\delta = \mathrm{tr}_1^n(ba^{-1})$. Then $L^0_{a,b,\delta}(u) = 0$ defined by (16) has at most four roots in $\mathbb{F}_{2^n}$.*

Proof. This can be proved completely the same as Proposition 2.

Theorem 2. *The Walsh spectrum of the function F_0 defined by (1) is $\{0, \pm 2^{(n+1)/2}\}$ if n is odd and $\{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}$ otherwise.*

Proof. The Walsh transform of F_0 takes values from $\{0, \pm 2^{(n+1)/2}\}$ if n is odd and takes values from $\{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}$ if n is even. This follows from (17) and Proposition 4. The Walsh transform takes all three values for n odd and all 5 values for n even by the same reasons as in Theorem 1.

4 Equivalence of Göloğlu's APN Trinomial to Gold Functions

In this section we prove that the function G defined by (4) is affine equivalent to the Gold function $x^{2^{m-k}+1}$. Note first that

$$G(x) = x^{2^m(2^k+1)} + x^{2^k+2^m} + x^{2^{m+k}+1},$$

and it is affine equivalent to the function

$$G'(x) = \big(G(x)\big)^{2^m} = x^{2^k+1} + x^{2^k+2^m} + x^{2^{m+k}+1}.$$

Linear functions

$$\begin{aligned} L_1(x) &= \gamma^{2^k} x^{2^{m+k}} + \gamma x^{2^k}, \\ L_2(x) &= \gamma x^{2^m} + \gamma^{2^k} x, \end{aligned}$$

where γ is a primitive element of $\mathbb{F}_{2^2}$, are permutations. Indeed, it is easy to see that the equations $L_1(x) = 0$ and $L_2(x) = 0$ have only 0 as a solution. Note that $L_1(x) = 0$ implies $L_1(x)^{2^m} = 0$ which give

$$\begin{aligned} \gamma^{2^k} x^{2^{m+k}} &= \gamma x^{2^k}, \\ \gamma^{2^{m+k}} x^{2^k} &= \gamma^{2^m} x^{2^{m+k}}. \end{aligned}$$

Hence, assuming $x \neq 0$ and multiplying both sides of the equalities above gives $\gamma^{2^k+2^{m+k}} = \gamma^{2^m+1}$ or $\gamma = \gamma^2$ (see explanation below) contradicting that γ is primitive in $\mathbb{F}_{2^2}$. The proof for L_2 being a permutation is similar.

Further we have

$$\begin{aligned} \big(L_1(x)\big)^{2^{m-k}+1} &= \gamma^{2^m+2^k} x^{2^{m+k}+1} + \gamma^{2^{m-k}+1} x^{2^m+2^k} + \gamma^{2^{m-k}+2^k} x^{2^{m+k}+2^m} + \gamma^{2^m+1} x^{2^k+1} \\ &= x^{2^{m+k}+1} + x^{2^m+2^k} + \gamma x^{2^{m+k}+2^m} + \gamma^2 x^{2^k+1} \end{aligned}$$

and

$$\begin{aligned} L_2 \circ G'(x) &= \gamma\big(x^{2^k+1} + x^{2^k+2^m} + x^{2^{m+k}+1}\big)^{2^m} + \gamma^{2^k}\big(x^{2^k+1} + x^{2^k+2^m} + x^{2^{m+k}+1}\big) \\ &= \big(\gamma + \gamma^{2^k}\big)\big(x^{2^{m+k}+1} + x^{2^m+2^k}\big) + \gamma x^{2^{m+k}+2^m} + \gamma^{2^k} x^{2^k+1} \\ &= x^{2^{m+k}+1} + x^{2^m+2^k} + \gamma x^{2^{m+k}+2^m} + \gamma^2 x^{2^k+1} \end{aligned}$$

since $\gcd(k, n) = 1$, $n = 2m = 4t$, and then

$$\begin{aligned} \gamma + \gamma^{2^k} &= \gamma + \gamma^2 = 1, \\ \gamma^{2^m+2^k} &= \gamma^{2^{m-k}+1} = \gamma^3 = 1, \\ \gamma^{2^{m-k}+2^k} &= \gamma^{2^k+2^{m+k}} = \gamma^4 = \gamma, \\ \gamma^{2^m+1} &= \gamma^2. \end{aligned}$$

Hence $\big(L_1(x)\big)^{2^{m-k}+1} = L_2 \circ G'(x) = L_2' \circ G(x)$ where $L_2'(x) = L_2(x^{2^m})$ is, obviously, a linear permutation. Therefore $x^{2^{m-k}+1}$ and G are affine equivalent.

Table 3. CCZ-inequivalent APN functions over $\mathbb{F}_{2^n}$ from the known APN classes ($6 \leq n \leq 11$ and a primitive in $\mathbb{F}_{2^n}$).

n	N°	Functions	Families from Tables 1 and 2	Relation to [27]
6	6.1	x^3	Gold	Table 5: $N^\circ 1.1$
	6.2	$x^6 + x^9 + a^7 x^{48}$	$N^\circ 3$	5: $N^\circ 1.2$
	6.3	$ax^3 + a^4 x^{24} + x^{17}$	$N^\circ 8$-10	5: $N^\circ 2.3$
7	7.1	x^3	Gold	Table 7 : $N^\circ 1.1$
	7.2	x^5	Gold	7 : $N^\circ 3.1$
	7.3	x^9	Gold	7 : $N^\circ 4.1$
	7.4	x^{13}	Kasami	7 : $N^\circ 5.1$
	7.5	x^{57}	Kasami	7 : $N^\circ 6.1$
	7.6	x^{63}	Inverse	7 : $N^\circ 7.1$
	7.7	$x^3 + \mathrm{tr}_1^7(x^9)$	$N^\circ 5$	7 : $N^\circ 1.2$
8	8.1	x^3	Gold	Table 9 : $N^\circ 1.1$
	8.2	x^9	Gold	9 : $N^\circ 1.2$
	8.3	x^{57}	Kasami	9 : $N^\circ 7.1$
	8.4	$x^3 + x^{17} + a^{48}x^{18} + a^3 x^{33} + ax^{34} + x^{48}$	$N^\circ 4$	9 : $N^\circ 2.1$
	8.5	$x^3 + \mathrm{tr}_1^8(x^9)$	$N^\circ 5$	9 : $N^\circ 1.3$
	8.6	$x^3 + a^{-1}\mathrm{tr}_1^8(a^3 x^9)$	$N^\circ 5$	9 : $N^\circ 1.5$
9	9.1	x^3	Gold	
	9.2	x^5	Gold	
	9.3	x^{17}	Gold	
	9.4	x^{13}	Kasami	
	9.5	x^{241}	Kasami	
	9.6	x^{19}	Welch	
	9.7	x^{255}	Inverse	
	9.8	$x^3 + \mathrm{tr}_1^9(x^9)$	$N^\circ 5$	
	9.9	$x^3 + \mathrm{tr}_3^9(x^9 + x^{18})$	$N^\circ 6$	
	9.10	$x^3 + \mathrm{tr}_3^9(x^{18} + x^{36})$	$N^\circ 7$	
10	10.1	x^3	Gold	
	10.2	x^9	Gold	
	10.3	x^{57}	Kasami	
	10.4	x^{339}	Dobbertin	
	10.5	$x^6 + x^{33} + a^{31}x^{192}$	$N^\circ 3$	
	10.6	$x^{72} + x^{33} + a^{31}x^{258}$	$N^\circ 3$	
	10.7	$x^3 + \mathrm{tr}_1^{10}(x^9)$	$N^\circ 5$	
	10.8	$x^3 + a^{-1}\mathrm{tr}_1^{10}(a^3 x^9)$	$N^\circ 5$	
11	11.1	x^3	Gold	
	11.2	x^5	Gold	
	11.3	x^9	Gold	
	11.4	x^{17}	Gold	
	11.5	x^{33}	Gold	
	11.6	x^{13}	Kasami	
	11.7	x^{57}	Kasami	
	11.8	x^{241}	Kasami	
	11.9	x^{993}	Kasami	
	11.10	x^{35}	Welch	
	11.11	x^{287}	Niho	
	11.12	x^{1023}	Inverse	
	11.13	$x^3 + \mathrm{tr}_1^{11}(x^9)$	$N^\circ 5$	

Proposition 5. *Let k, n, m, t be positive integers such that $\gcd(k, n) = 1$, $n = 2m = 4t$. Then the function G defined by (4) and the function $x^{2^{m-k}+1}$ over $\mathbb{F}_{2^n}$ are affine equivalent.*

Remark 1. *For $k = 1$ the APN function G and its equivalence to Gold functions were known from [14].*

We note that it is possible to check CCZ-equivalence of functions with a computer for n up to 12. However, since most of the known families of APN functions are defined for many different parameters and coefficients it becomes extremely difficult to check CCZ-equivalence of a given function to all of them. For this reason we tested all possible parameters and coefficients to produce Table 3 of all CCZ-inequivalent functions arising from the known infinite families of APN functions for $n \leq 11$.

References

1. Beth, T., Ding, C.: On almost perfect nonlinear permutations. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 65–76. Springer, Heidelberg (1994). doi:10.1007/3-540-48285-7_7
2. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptology **4**(1), 3–72 (1991)
3. Bracken, C., Byrne, E., Markin, N., McGuire, G.: A few more quadratic APN functions. Crypt. Commun. **3**(1), 43–53 (2011)
4. Bracken, C., Byrne, E., Markin, N., McGuire, G.: New families of quadratic almost perfect nonlinear trinomials and multinomials. Finite Fields Appl. **14**(3), 703–714 (2008)
5. Bracken, C., Byrne, E., Markin, N., McGuire, G.: On the Walsh spectrum of a new APN function. In: Galbraith, S.D. (ed.) Cryptography and Coding 2007. LNCS, vol. 4887, pp. 92–98. Springer, Heidelberg (2007). doi:10.1007/978-3-540-77272-9_6
6. Bracken, C., Byrne, E., Markin, N., McGuire, G.: On the Fourier spectrum of binomial APN functions. SIAM J. Discrete Math. **23**(2), 596–608 (2009)
7. Bracken, C., Byrne, E., Markin, N., McGuire, G.: Determining the nonlinearity of a new family of APN functions. In: Boztaş, S., Lu, H.-F.F. (eds.) AAECC 2007. LNCS, vol. 4851, pp. 72–79. Springer, Heidelberg (2007). doi:10.1007/978-3-540-77224-8_11
8. Bracken, C., Zha, Z.: On the Fourier spectra of the infinite families of quadratic APN functions. Finite Fields Appl. **18**(3), 537–546 (2012)
9. Brinkmann, M., Leander, G.: On the classification of APN functions up to dimension five. Des. Codes Crypt. **49**(1–3), 273–288 (2008)
10. Browning, A.K., Dillon, F.J., Kibler, E.R., McQuistan, T.M.: APN polynomials and related codes. J. Comb. Inf. Syst. Sci. **34**(1–4), 135–159 (2009). Special Issue in Honor of Prof. D.K Ray-Chaudhuri on the occasion of his 75th birthday
11. Browning, A.K., Dillon, F.J., McQuistan, T.M., Wolfe, J.A.: An APN permutation in dimension six. In: Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications Fq 2009, Contemporary Math, AMS, vol. 518, pp. 33–42 (2010)
12. Budaghyan, L., Carlet, C.: Classes of quadratic APN trinomials and hexanomials and related structures. IEEE Trans. Inform. Theor. **54**(5), 2354–2357 (2008)

13. Budaghyan, L., Carlet, C., Leander, G.: Two classes of quadratic APN binomials inequivalent to power functions. IEEE Trans. Inform. Theor. **54**(9), 4218–4229 (2008)
14. Budaghyan, L., Carlet, C., Leander, G.: Constructing new APN functions from known ones. Finite Fields Appl. **15**(2), 150–159 (2009)
15. Budaghyan, L., Carlet, C., Leander, G.: On a construction of quadratic APN functions. In: IEEE Information Theory Workshop, pp. 374–378 (2009)
16. Budaghyan, L., Carlet, C., Pott, A.: New classes of almost bent and almost perfect nonlinear functions. IEEE Trans. Inform. Theor. **52**(3), 1141–1152 (2006)
17. Canteaut, A., Charpin, P., Dobbertin, H.: Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture. IEEE Trans. Inform. Theor. **46**(1), 4–8 (2000)
18. Carlet, C.: Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. Des. Codes Crypt. **59**(1–3), 89–109 (2011)
19. Carlet, C.: Vectorial Boolean functions for cryptography. In: Crama, Y., Hammer, P. (eds.) Boolean Methods and Models. Cambridge University Press (2005–2006, to appear). Chapter of the Monography
20. Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Crypt. **15**(2), 125–156 (1998)
21. Chabaud, F., Vaudenay, S.: Links between differential and linear cryptanalysis. In: Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 356–365. Springer, Heidelberg (1995). doi:10.1007/BFb0053450
22. Dobbertin, H.: Almost perfect nonlinear power functions over $GF(2^n)$: the Niho case. Inform. Comput. **151**, 57–72 (1999)
23. Dobbertin, H.: Almost perfect nonlinear power functions over $GF(2^n)$: the Welch case. IEEE Trans. Inform. Theor. **45**, 1271–1275 (1999)
24. Dobbertin, H.: Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5. In: Proceedings of Finite Fields and Applications Fq5, pp. 113–121 (2000)
25. Dobbertin, H.: Another proof of Kasami's theorem. Des. Codes Crypt. **17**, 177–180 (1999)
26. Edel, Y.: Quadratic APN functions as subspaces of alternating bilinear forms. In: Contact Forum Coding Theory and Cryptography III 2009, Belgium, pp. 11–24 (2011)
27. Edel, Y., Pott, A.: A new almost perfect nonlinear function which is not quadratic. Adv. Math. Commun. **3**(1), 59–81 (2009)
28. Gold, R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inform. Theor. **14**, 154–156 (1968)
29. Göloğlu, F.: Almost perfect nonlinear trinomials and hexanomials. Finite Fields Appl. **33**, 258–282 (2015)
30. Hollmann, H., Xiang, Q.: A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences. Finite Fields Appl. **7**, 253–286 (2001)
31. Janwa, H., Wilson, R.M.: Hyperplane sections of fermat varieties in P^3 in char. 2 and some applications to cyclic codes. In: Cohen, G., Mora, T., Moreno, O. (eds.) AAECC 1993. LNCS, vol. 673, pp. 180–194. Springer, Heidelberg (1993). doi:10.1007/3-540-56686-4_43
32. Kasami, T.: The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes. Inform. Control **18**, 369–394 (1971)
33. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994). doi:10.1007/3-540-48285-7_33

34. Nyberg, K.: Differentially uniform mappings for cryptography. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 55–64. Springer, Heidelberg (1994). doi:10.1007/3-540-48285-7_6
35. Nyberg, K.: Perfect nonlinear S-boxes. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 378–386. Springer, Heidelberg (1991). doi:10.1007/3-540-46416-6_32
36. Tan, Y., Qu, L., Ling, S., Tan, C.H.: On the Fourier spectra of new APN functions. SIAM J. Discrete Math. **27**(2), 791–801 (2013)
37. Yu, Y., Wang, M., Li, Y.: A matrix approach for constructing quadratic APN functions. In: Pre-proceedings of the International Conference WCC 2013, Bergen, Norway (2013)