Generalized Isotopic Shift Construction for APN Functions*

Lilya Budaghyan[a], Marco Calderini[a], Claude Carlet[a,b], Robert Coulter[c], Irene Villa[a]

[a] *University of Bergen, Bergen, Norway*
[b] *LAGA, University of Paris 8, Paris, France*
[c] *The University of Delaware, Newark, Delaware USA*

Abstract

In this work we give several generalizations of the isotopic shift construction, introduced recently by Budaghyan et al. (2018), when the starting function is a Gold function. In particular, we derive a general construction of APN functions which produces one new APN function for $n = 8$ and fifteen new APN functions for $n = 9$.

Keywords: APN functions, Isotopic shift, Vectorial Boolean functions.
MSC: 94A60, 06E30, 11T71

1. Introduction

For n a positive integer, let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements. By $\mathbb{F}_{2^n}^\star$ we denote the multiplicative group of $\mathbb{F}_{2^n}$ and, throughout the paper, ζ denotes one of its primitive elements, so that $\mathbb{F}_{2^n}^\star = \langle\zeta\rangle = \{1, \zeta, \zeta^2, \zeta^3, \ldots, \zeta^{2^n-2}\}$. An (n, n)-function is a map from $\mathbb{F}_{2^n}$ to itself. Such a function admits a unique representation as a univariate polynomial of degree at most $2^n - 1$, that is

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

The kernel of F is defined as $\ker(F) = \{u \in \mathbb{F}_{2^n} \ s.t. \ F(u) = 0\}$.

The function F is

- *linear* if $F(x) = \sum_{i=0}^{n-1} c_i x^{2^i}$;
- *affine* if it is the sum of a linear function and a constant;
- *DO* (Dembowski-Ostrom) *polynomial* if $F(x) = \sum_{0\le i<j<n} a_{ij} x^{2^i+2^j}$, with $a_{ij} \in \mathbb{F}_{2^n}$;

*Parts of this work were presented at *WCC 2019 : The Eleventh International Workshop on Coding and Cryptography.*

**Corresponding author: Irene Villa, with the Department of Informatics, University of Bergen, N-5020 Bergen, Norway

Email addresses: Lilya.Budaghyan@uib.no (Lilya Budaghyan), Marco.Calderini@uib.no (Marco Calderini), claude.carlet@gmail.com (Claude Carlet), coulter@udel.edu (Robert Coulter), Irene.Villa@uib.no (Irene Villa)

- *quadratic* if it is the sum of a DO polynomial and an affine function.

A function F is called *differentially δ-uniform*, for δ a positive integer, if for any pair $(a, b) \in \mathbb{F}_{2^n}^2$, with $a \neq 0$, the equation $F(x + a) - F(x) = b$ admits at most δ solutions. When F is used as an S-box inside a cryptosystem, the differential uniformity measures its contribution to the resistance to the differential attack [3]. The smaller δ is, the better is the resistance to this attack.

Over fields of characteristic 2, the solutions of the equation $F(x+a)-F(x) = b$, that is, $F(x+a)+F(x) = b$, come in pairs $\{x, x+a\}$, and δ is even. The best resistance is then achieved by differentially 2-uniform functions. Such functions are also called *almost perfect nonlinear*; in short, APN. One of the best known examples of APN functions is Gold function, $\mathcal{G}_i(x) = x^{2^i+1}$, which is APN whenever i is coprime with n.

APN functions have connections to optimal objects in other fields such as geometry, sequence design and combinatorics.

There are several equivalence relations of functions for which differential uniformity, and thus the APN property, is preserved. Two functions F and F' from $\mathbb{F}_{2^n}$ to itself are called:

- *affine equivalent* if $F' = A_1 \circ F \circ A_2$ where $A_1, A_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are affine permutations;
- *EA-equivalent* if $F' = F'' + A$, where the map $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is affine and F'' is affine equivalent to F;
- *CCZ-equivalent* if there exists some affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that the image of the graph of F is the graph of F', that is, $\mathcal{L}(G_F) = G_{F'}$, where $G_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ and $G_{F'} = \{(x, F'(x)) : x \in \mathbb{F}_{2^n}\}$.

CCZ-equivalence is the most general known equivalence relation for functions which preserves differential uniformity, while affine and EA-equivalences are particular cases.

Inspired by the notion of *isotopic equivalence*, originally defined by Albert [1] in the study of presemifields and semifields, a new construction method for APN functions, called isotopic shift, was introduced in [5].

More precisely, given p a prime number, $F \in \mathbb{F}_{p^n}[x]$ a function, and $L \in \mathbb{F}_{p^n}[x]$ a linear map, the *isotopic shift* of F by L is defined as the map:

$$F_L(x) = F(x + L(x)) - F(x) - F(L(x)). \tag{1}$$

As we have shown in [5], for the case $p = 2$, an isotopic shift of an APN function can lead to APN functions CCZ-inequivalent to the original map. In particular, all existing quadratic APN functions over $\mathbb{F}_{2^6}$, which are 13 up to CCZ-equivalence, can be obtained from x^3 by isotopic shift. Moreover, a new family of quadratic APN functions, which generates a new APN function for $n = 9$, is constructed by isotopic shift of Gold functions [5]. In [6], the isotopic shift construction has been investigated for the case of planar functions ($p > 2$), i.e. differentially 1-uniform functions. Also here, given a planar function, it is

possible to obtain an inequivalent planar function from its isotopic shifts.

In the present paper we further study the isotopic shift construction over fields of even characteristic. Firstly, we verify that, over $\mathbb{F}_{2^6}$, any quadratic APN map can be obtained as an isotopic shift of any other quadratic APN map. Then, we consider different generalizations of the isotopic shift construction when the starting function is a monomial with a Gold exponent. In [5], we studied the APN property of the isotopic shift of $\mathcal{G}_i(x) = x^{2^i+1}$ over $\mathbb{F}_{2^n}$, with $n = km$, given by

$$\mathcal{G}_{i,L}(x) = xL(x)^{2^i} + x^{2^i}L(x), \tag{2}$$

where L is a 2^m-polynomial, that is $L(x) = \sum_{i=0}^{k-1} A_i x^{2^{im}}$ for some $A_i \in \mathbb{F}_{2^n}$. This construction provides a new APN function over $\mathbb{F}_{2^9}$.

In the present work, we study the APN property of $xL_1(x)^{2^i} + x^{2^i}L_2(x)$ where both L_1 and L_2 are 2^m-polynomials. From this construction, we obtain one new APN function for $n = 8$, and fifteen for $n = 9$. Moreover, we cover some of the functions in the lists given in [13] which are not contained in any of the known infinite families. In 2014, a matrix construction for quadratic APN functions was presented that led to a list of 8180 CCZ-inequivalent quadratic APN functions over $\mathbb{F}_{2^8}$, see [20]. By obtaining a new quadratic APN map, we show that the list was not complete.

To show the inequivalence between some of the obtained maps, we introduce in Proposition 3.4 a new EA-invariant (this invariant was also noticed independently in [14]). Note that for quadratic APN functions, CCZ-equivalence coincides with EA-equivalence [19].

Finally, we consider the case when the isotopic shift of $\mathcal{G}_i(x)$ is obtained using a function L not necessarily linear. In this case we find that all known power APN functions in odd dimension, except the Dobbertin function, can be obtained as nonlinear shifts of Gold functions.

2. Further results on the isotopic linear shift over $\mathbb{F}_{2^n}$

Before considering generalizations of the isotopic shift, we extend a result obtained in [5].

We have shown that, given a quadratic APN function F, if the isotopic shift F_L by a linear map L is APN, then the map L is either a permutation or a 2-to-1 map. From the isotopic shifts of the Gold function x^3, with both choices for L being a permutation and a 2-to-1 map, we obtained (computationally) all the quadratic APN functions over $\mathbb{F}_{2^6}$ (up to EA-equivalence). That is, for any given quadratic APN function F over $\mathbb{F}_{2^6}$ there exist a permutation L and a 2-to-1 map L' such that the isotopic shifts $\mathcal{G}_{1,L}(x)$ and $\mathcal{G}_{1,L'}(x)$ are EA-equivalent to F. The same result was computationally obtained for any quadratic APN map over $\mathbb{F}_{2^6}$ listed in [13, Table 5] (see also [4]) in place of $\mathcal{G}_1$. Up to EA-equivalence (and thus CCZ-equivalence) the list is complete and, since for two quadratic maps the EA-equivalence implies EA-equivalence of the isotopic shifts (see [5, Corollary 3.2]), we can state the following result.

Proposition 2.1. *Over $\mathbb{F}_{2^6}$ for any two quadratic APN maps F and G, there exist a linear permutation L and a linear 2-to-1 map L' such that F_L and $F_{L'}$ are EA-equivalent to G.*

We conclude with the observation that the isotopic shift can lead to an APN function also starting from a non-APN function.

Remark 2.2. *Consider $\mathbb{F}_{2^6}$ and the function $F(x) = x^5$, which is not APN. With $L(x) = \zeta x^8$ we construct the APN map*

$$F_L(x) = x^4 L(x) + xL(x)^4 = \zeta x^{12} + \zeta^4 x^{33},$$

where $F_L(x) = M(x^3)$ for the linear permutation $M(x) = \zeta x^4 + \zeta^4 x^{32}$.

3. Generalized isotopic shift of Gold functions

In this section we generalize the isotopic shift construction for the case of Gold functions.

3.1. On the generalized linear shift over $\mathbb{F}_{2^n}$

In [5], we showed that the isotopic shift can be a useful construction method for APN functions. Let $n = km$, where m and k are any positive integers. An $\mathbb{F}_{2^m}$-polynomial is a linear map given by $L(x) = \sum_{j=0}^{k-1} A_j x^{2^{jm}}$, for some $A_j \in \mathbb{F}_{2^n}$. The construction $\mathcal{G}_{i,L}(x)$ as in (2) leads to a family of APN functions, producing, in particular, for $n = 9$ $(k, m = 3)$ a new APN function and for $n = 8$ $(k = 4,\ m = 2)$ a function equivalent to $x^9 + \mathrm{Tr}(x^3)$, which is not contained in any infinite family.

In the following, we generalize the isotopic shift construction. This generalization provides further new APN functions, as will be shown below.

Given two positive integers k, m, let us consider the finite field $\mathbb{F}_{2^n}$ with $n = km$. Denoting $d = \gcd(2^m - 1, \frac{2^{km}-1}{2^m-1})$, let d' be the positive integer with the same prime factors as d , satisfying $\gcd(2^m - 1, \frac{2^{km}-1}{(2^m-1)d'}) = 1$. Now, let $U = \langle \zeta^{d'(2^m-1)} \rangle$ be the multiplicative subgroup of $\mathbb{F}_{2^n}^\star$ of order $\left(\frac{2^{km}-1}{2^m-1}\right)/d'$. Note that it is possible to write every element $x \in \mathbb{F}_{2^n}^\star$ as $x = ut$ with $u \in W$ and $t \in \mathbb{F}_{2^m}^\star$, where $W = \{\zeta^s y : y \in U,\ 0 \le s \le d' - 1\}$.
Then it is possible to obtain the following generalization of [5, Theorem 6.3].

Theorem 3.1. *Let $n = km$ for $m > 1$. Let $L_1(x) = \sum_{j=0}^{k-1} A_j x^{2^{jm}}$ and $L_2(x) = \sum_{j=0}^{k-1} B_j x^{2^{jm}}$ be two $\mathbb{F}_{2^m}$-polynomials. Fix i so that $\gcd(i, m) = 1$ and $F \in \mathbb{F}_{2^n}[x]$ the function given by:*

$$F(x) = xL_1(x)^{2^i} + x^{2^i} L_2(x). \tag{3}$$

Then F is APN over $\mathbb{F}_{2^n}$ if and only if each of the following statements holds for any $v \in W$:

- $(\frac{L_1(v)}{v})^{2^i} \neq \frac{L_2(v)}{v}$;
- *If $u \in W \setminus \{1\}$ and $(\frac{L_1(uv)}{uv})^{2^i} = \frac{L_2(v)}{v}$, then $(\frac{L_1(v)}{v})^{2^i} \neq \frac{L_2(uv)}{uv}$;*
- *If $u \in W \setminus \{1\}$ and $(\frac{L_1(uv)}{uv})^{2^i} \neq \frac{L_2(v)}{v}$, then $\frac{L_1(v)^{2^i}(uv) + L_2(uv)v^{2^i}}{L_1(uv)^{2^i} v + L_2(v)(uv)^{2^i}} \notin \mathbb{F}_{2^m}^\star$.*

Proof. We need that, for any $a \in \mathbb{F}_{2^n}^\star$, the function $\Delta_a(x) = F(x+a) + F(x) + F(a)$ is a 2-to-1 map, or equivalently, that $\ker(\Delta_a(ax)) = \{0,1\}$. Since $\mathbb{F}_{2^n}^\star = W \times \mathbb{F}_{2^m}^\star$, we can rewrite $a = st$ and $x = uv$ with $s, u \in \mathbb{F}_{2^m}^\star$ and $t, v \in W$. Since L_1 and L_2 are $\mathbb{F}_{2^m}$-polynomials, we have:

$$\begin{aligned}\Delta_a(ax) =& L_1(a)^{2^i} ax + L_2(a)(ax)^{2^i} + L_1(ax)^{2^i} a + L_2(ax)a^{2^i} \\ =& s^{2^i} L_1(t)^{2^i} st \cdot uv + sL_2(t)s^{2^i} t^{2^i} \cdot u^{2^i} v^{2^i} + s^{2^i} u^{2^i} L_1(tv)^{2^i} st + suL_2(tv)s^{2^i} t^{2^i} \\ =& us^{2^i+1}[(L_1(t)^{2^i} tv + L_2(tv)t^{2^i}) + u^{2^i-1}(L_2(t)t^{2^i} v^{2^i} + L_1(tv)^{2^i} t)].\end{aligned}$$

Without loss of generality we can assume that $s = 1$. So, F is APN over $\mathbb{F}_{2^n}$ if and only if $u = 0$ or $u = v = 1$ are the only solutions to $\Delta_t(uvt) = 0$ for any $t \in U$.

If $v = 1$, then

$$\Delta_t(tx) = u(L_1(t)^{2^i} t + L_2(t)t^{2^i})[1 + u^{2^i-1}].$$

Since $\gcd(i, m) = 1$, x^{2^i-1} is a permutation over $\mathbb{F}_{2^m}$ and thus $\ker(\Delta_t(tx)) = \{0,1\}$ if and only if $\frac{L_1(t)^{2^i}}{t^{2^i}} \neq \frac{L_2(t)}{t}$.

Assume now that $v \neq 1$. If $L_2(t)t^{2^i} v^{2^i} + L_1(tv)^{2^i} t = 0$, then we have:

$$\Delta_t(tx) = u[(L_1(t)^{2^i} tv + L_2(tv)t^{2^i})].$$

This implies $\frac{L_1(t)^{2^i}}{t^{2^i}} \neq \frac{L_2(tv)}{tv}$.

If $L_2(t)t^{2^i} v^{2^i} + L_1(tv)^{2^i} t \neq 0$, then

$$[(L_1(t)^{2^i} tv + L_2(tv)t^{2^i}) + u^{2^i-1}(L_2(t)t^{2^i} v^{2^i} + L_1(tv)^{2^i} t)] = 0$$

implies $u^{2^i-1} = \frac{L_1(t)^{2^i} tv + L_2(tv)t^{2^i}}{L_2(t)t^{2^i} v^{2^i} + L_1(tv)^{2^i} t}$. Since x^{2^i-1} is a permutation over $\mathbb{F}_{2^m}$ this equation admits a solution different from zero if and only if $\frac{L_1(t)^{2^i} tv + L_2(tv)t^{2^i}}{L_2(t)t^{2^i} v^{2^i} + L_1(tv)^{2^i} t}$ is contained in $\mathbb{F}_{2^m}^\star$. □

The obtained APN function (3) is of the form

$$F(x) = (A_0^{2^i} + B_0)x^{2^i+1} + \sum_{j=1}^{k-1} [A_j^{2^i} x^{2^{i+jm}+1} + B_j x^{2^{jm}+2^i}].$$

Let us see now necessary conditions on the linear functions L_1 and L_2 for F to be APN.

Proposition 3.2. *Let n, L_1, L_2 and F be as in Theorem 3.1. If F is APN over $\mathbb{F}_{2^n}$, then the following statements hold:*

(i) $\ker(L_1(x) + rx) \cap \ker(L_2(x) + r^{2^i} x) = \{0\}$ *for any* $r \in \mathbb{F}_{2^n}$*;*
(ii) $|\ker(L_1(x)^{2^i} + rx) \cap \ker(L_2(x) + w^{2^i} x^{2^i})| \leq 2$ *for any* $r, w \in \mathbb{F}_{2^n}$*;*
(iii) *If* $\ker(L_1) \cap \ker(L_2(x) + x) \neq \{0\}$*, then* $\ker(L_1(x) + x) \cap \ker(L_2) = \{0\}$*;*
(iv) $\ker(L_1(x) + rx^{2^j}) \cap \ker(L_2(x) + r^{2^i} x^{(2^j-1)2^i+1}) = \{0\}$ *for any* $r \in \mathbb{F}_{2^n}$ *and* $j \geq 0$.

Proof. For any nonzero a, we define the function $\Delta_a(x) = F(x+a)+F(x)+F(a)$. Suppose there exists a non-zero $a \in \ker(L_1(x) + rx) \cap \ker(L_2(x) + r^{2^i}x)$. As

$$\Delta_a(x) = aL_1(x)^{2^i} + xL_1(a)^{2^i} + x^{2^i}L_2(a) + a^{2^i}L_2(x),$$

we clearly have $a\mathbb{F}_{2^m} \subseteq \ker(\Delta_a)$, but since $m > 1$, this contradicts $|\ker(\Delta_a)| = 2$. This establishes (i).

For (ii), suppose $\{0, a, b\} \subset \ker(L_1(x)^{2^i} + rx) \cap \ker(L_2(x) + w^{2^i}x^{2^i})$. Then

$$\Delta_a(b) = a(rb) + b(ra) + a^{2^i}(w^{2^i}b^{2^i}) + b^{2^i}(w^{2^i}a^{2^i}) = 0.$$

Next suppose $a \in \ker(L_1) \cap \ker(L_2(x)+x)$. Then we have $\Delta_a(x) = a(L_1(x)+x)^{2^i} + a^{2^i}L_2(x)$. Clearly any $b \in \ker(L_1(x) + x) \cap \ker(L_2)$ satisfies $\Delta_a(b) = 0$. Since f is APN, $\ker(\Delta_a) = \{0, a\}$, so that $\ker(L_1(x) + x) \cap \ker(L_2) \subset \{0, a\}$. However, $\ker(L_1) \cap \ker(L_1(x) + x) = \{0\}$, so that no non-zero element of $\mathbb{F}_{2^n}$ can lie in both $\ker(L_1) \cap \ker(L_2(x) + x)$ and $\ker(L_1(x) + x) \cap \ker(L_2)$. This establishes (iii).

For (iv), suppose $a \in \ker(L_1(x) + rx^{2^j}) \cap \ker(L_2(x) + r^{2^i}x^{(2^j-1)2^i+1})$ is non-zero. Then for any $t \in \mathbb{F}_{2^m}$ we have

$$\begin{aligned}\Delta_a(ta) &= ar^{2^i}t^{2^i}a^{2^{j+i}} + tar^{2^i}a^{2^{j+i}} + (ta)^{2^i}r^{2^i}a^{(2^j-1)2^i+1} + a^{2^i}r^{2^i}ta^{(2^j-1)2^i+1} \\ &= r^{2^i}a^{2^{j+i}+1}\left(t^{2^i} + t + t^{2^i} + t\right) = 0,\end{aligned}$$

so that $a\mathbb{F}_{2^m} \subseteq \ker(\Delta_a)$, a contradiction. □

3.2. The case $n = 8$

Applying the construction of Theorem 3.1 in dimension 8 with $k = 4$ and $m = 2$, restricting the coefficients of L_1 and L_2 to the subfield $\mathbb{F}_{2^4}$ we obtained one new APN function CCZ-inequivalent to any of the 8180 APN functions known (see Appendix in [20] for a complete list[1] of all APN functions). Moreover, this construction leads to several APN functions given in [13, Table 9] which have not been previously identified as a part of any APN family. The functions mentioned are listed in Table 1.

The following results were obtained for $n = 8$.

- A new function was found as generalized isotopic shift of x^3,

  $$F(x) = \zeta^{136}x^{66} + \zeta^{85}x^{33} + \zeta^{85}x^{18} + \zeta^{102}x^9 + \zeta^{221}x^6 + x^3,$$

  where $L_1(x) = \zeta^{170}x^{16} + \zeta^{102}x^4 + x$ and $L_2(x) = \zeta^{136}x^{64} + \zeta^{85}x^{16} + \zeta^{221}x^4$, with the following CCZ-invariants Γ-rank=14034, Δ-rank=438 and $|\mathcal{M}_{G_F}| = 2^{10} \cdot 3$ (see [13] for more details on these invariants).
- Considering generalized isotopic shifts of x^3 it is possible to obtain maps EA-equivalent to nos. 1.2, 1.5, 1.7, 1.8, 1.10, 1.11, 1.12, 1.16, 1.17, 3.1 in Table 9 [13].
- Considering generalized isotopic shifts of x^9 it is also possible to obtain maps EA-equivalent to no. 1.3 in the same table.

[1] An up-to-date table can also be found at `https://boolean.h.uib.no/mediawiki/index.php/Known\_quadratic\_APN\_polynomial\_functions\_over\_GF(2\^{}8)`

Table 1: APN polynomials over $\mathbb{F}_{2^8}$ derived from Theorem 3.1. All are either new or correspond to the known but unclassified cases.

Functions	equiv. to no. in Table 9 in [13]
$\zeta^{136}x^{66}+\zeta^{85}x^{33}+\zeta^{85}x^{18}+\zeta^{102}x^{9}+\zeta^{221}x^{6}+x^{3}$	New
$\zeta^{102}x^{66}+\zeta^{204}x^{9}+x^{3}$	1.2
$\zeta^{153}x^{129}+\zeta^{204}x^{66}+\zeta^{170}x^{33}+\zeta^{85}x^{18}+\zeta^{204}x^{6}+x^{3}$	1.5
$\zeta^{102}x^{129}+\zeta^{153}x^{66}+\zeta^{170}x^{33}+\zeta^{221}x^{18}+\zeta^{221}x^{9}+\zeta^{187}x^{6}+x^{3}$	1.7
$x^{66}+\zeta^{85}x^{33}+x^{18}+x^{9}+x^{3}$	1.8
$\zeta^{204}x^{129}+\zeta^{170}x^{66}+\zeta^{153}x^{33}+\zeta^{85}x^{18}+\zeta^{153}x^{9}+\zeta^{17}x^{6}+x^{3}$	1.10
$\zeta^{204}x^{66}+x^{33}+x^{18}+\zeta^{153}x^{9}+x^{3}$	1.11
$\zeta^{170}x^{129}+\zeta^{204}x^{66}+\zeta^{17}x^{33}+\zeta^{68}x^{18}+\zeta^{221}x^{9}+\zeta^{204}x^{6}+x^{3}$	1.12
$\zeta^{238}x^{129}+\zeta^{204}x^{66}+\zeta^{119}x^{33}+\zeta^{68}x^{18}+\zeta^{85}x^{9}+\zeta^{119}x^{6}+x^{3}$	1.16
$\zeta^{17}x^{129}+\zeta^{85}x^{66}+\zeta^{34}x^{33}+\zeta^{34}x^{18}+\zeta^{187}x^{9}+\zeta^{187}x^{6}+x^{3}$	1.17
$\zeta^{17}x^{129}+\zeta^{238}x^{66}+\zeta^{153}x^{33}+\zeta^{85}x^{18}+\zeta^{238}x^{9}+\zeta^{102}x^{6}+x^{3}$	3.1
$\zeta^{153}x^{129}+\zeta^{221}x^{72}+\zeta^{170}x^{33}+\zeta^{102}x^{24}+x^{12}+x^{9}+\zeta^{136}x^{3}$	1.3

Remark 3.3. *The new function has the same CCZ-invariants (Γ-rank, Δ-rank and $\mathcal{M}_{G_F}$) as function number 1.9 in Table 9 of [13].*
Since two quadratic APN functions are CCZ-equivalent if and only if they are EA-equivalent [19], the CCZ-inequivalence between these two functions can be obtained by checking another invariant with respect to the EA-equivalence that we shall introduce in the next subsection.

3.3. A new EA-equivalence invariant

Let $S(F)=\{b\in\mathbb{F}_{2^n} : \exists\, a\in\mathbb{F}_{2^n} \text{ s.t. } \mathcal{W}_F(a,b)=0\}$, where $\mathcal{W}_F(a,b)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(ax+bF(x))}$ is the Walsh coefficient of F in a and b. This set was used in [7] to study some relations between the CCZ-equivalence and the EA-equivalence.

It is easy to check that:

- if $F'(x)=F(x)+L(x)$ with L linear, then $b\in S(F)$ if and only if $b\in S(F')$.
- If $F'(x)=A_1\circ F\circ A_2(x)$ with A_1, A_2 affine permutations, then $b\in S(F)$ if and only if $\bar{A}_1^*(b)\in S(F')$, where $\bar{A}_1^*$ is the adjoint operator of the linear map $A_1(x)+A_1(0)$.

From this we have the following.

Proposition 3.4. *Let N_i be the number of the $\mathbb{F}_2$-vector subspaces of $\mathbb{F}_{2^n}$ contained in $S(F)$ of dimension i. Then, the values N_i for $i=1,...,n$ are EA-invariant.*

Proof. If F' is EA-equivalent to F, then there exist A_1, A_2 affine permutations and L linear such that $F'(x)=A_1\circ F\circ A_2(x)+L(x)$. From the arguments above, denoting $\bar{A}_1(x)=A_1(x)+A_1(0)$ we have that $S(F')=\bar{A}^*(S(F))$. □

Remark 3.5. *We computed the values N_i for the two functions and we got $N_1=86$, $N_2=340$ and $N_3=4$ for the new function, and $N_1=86$, $N_2=340$ and $N_3=8$ for the function number 1.9. Thus from Proposition 3.4 we have that the two functions are not EA-equivalent.*

Remark 3.6. *Note that when n is odd, a quadratic APN function F is Almost Bent (i.e. for all $b \in \mathbb{F}_{2^n}^\star$ we have $\{\mathcal{W}_F(a,b) : a \in \mathbb{F}_{2^n}\} = \{0, \pm 2^{(n+1)/2}\}$), which implies $S(F) = \mathbb{F}_{2^n}$. Thus, this new invariant cannot be used for testing the CCZ-equivalence of quadratic APN functions in the case n odd.*

Remark 3.7. *In fact, this EA-invariant was tackled independently by Göloğlu and Pavlů in [14]. In their work, they focused on plateaued functions and looked at the subspaces in the set $\{b : \mathcal{W}_F(0,b) \neq \pm 2^{n/2}\}$ (n even). For plateaued functions, this set coincides with $S(F)$.*

3.4. The case $n = 9$

For the case $k = m = 3$ we consider the generalized linear shift as in (3) with L_1 and L_2 having coefficients in the subfield $\mathbb{F}_{2^3}$. In Table 2 we list all known APN functions for $n = 9$, as reported in [5, Table 1]. In Table 3, we list all new APN functions obtained from Theorem 3.1. We observe that the family of Theorem 3.1 covers the only known example of an APN function for $n = 9$, function 8.1 of Table 11 in [13], which had not been previously identified as part of an APN family. Hence, currently, all known APN functions for $n = 9$ are now covered by an APN family. Note that this latter function was not obtained from the approach studied in [13] (it does not belong to a switching class of a previously known APN map). Finally, Table 3 indicates 15 new APN functions all obtained from Theorem 3.1. In both tables we include, for each function, the CCZ-invariants Γ-rank, Δ-rank and $|\mathcal{M}_{G_F}|$.

The CCZ-inequivalence of some of these functions was obtained by checking with MAGMA the equivalence of some linear code which can be associated to an APN function (see [4]).

Table 2: Previously known CCZ-inequivalent APN polynomials over $\mathbb{F}_{2^9}$ and their relation to previously known families of APN functions.

Functions	Families	no. Table 11 in [13]	Γ-rank	Δ-rank	$\lvert\mathcal{M}_{G_F}\rvert$
x^3	Gold	1.1	38470	872	$9 \cdot 2^9 \cdot 511$
x^5	Gold	2.1	41494	872	$9 \cdot 2^9 \cdot 511$
x^{17}	Gold	3.1	38470	872	$9 \cdot 2^9 \cdot 511$
x^{13}	Kasami	4.1	58676	3086	$9 \cdot 511$
x^{241}	Kasami	6.1	61726	3482	$9 \cdot 511$
x^{19}	Welch	5.1	60894	3956	$9 \cdot 511$
x^{255}	Inverse	7.1	130816	93024	$2 \cdot 9 \cdot 511$
$Tr_1^9(x^9) + x^3$	[8]	1.2	47890	920	$9 \cdot 2^9$
$Tr_3^9(x^{18} + x^9) + x^3$	[9]	1.3	48428	930	$9 \cdot 2^9$
$Tr_3^9(x^{36} + x^{18}) + x^3$	[9]	1.4	48460	944	$9 \cdot 2^9$
$x^3 + x^{10} + \zeta^{438}x^{136}$	–	8.1	48608	938	$3 \cdot 7 \cdot 2^9$
$\zeta^{337}x^{129} + \zeta^{424}x^{66} + \zeta^2 x^{17} + \zeta x^{10} + \zeta^{34}x^3$	[5]	–	48596	944	$3 \cdot 7 \cdot 2^9$

3.5. Isotopic shifts with nonlinear functions

In this section we consider the case when the function used in the shift is not necessarily linear.

In [5], it has been proved that, in even dimension, an isotopic shift of the Gold function with a linear function defined over $\mathbb{F}_2[x]$ cannot be APN. In the following, we show that for any quadratic function F in even dimension, we

Table 3: APN polynomials over $\mathbb{F}_{2^9}$ derived from Theorem 3.1. All, except for the first one, are either new or correspond to the one known but unclassified case.

$\mathcal{G}_i$	Function	Eq. to known ones	Γ-rank	Δ-rank	$\lvert\mathcal{M}_{G_F}\rvert$
$i=1$	$x^{129}+\zeta^{146}x^{66}+x^{17}+\zeta^{365}x^{10}+x^3$	eq. to APN function in [5]	48596	944	$2^9\cdot 3\cdot 7$
$i=1$	$\zeta^{219}x^{129}+\zeta^{292}x^{66}+\zeta^{292}x^{17}+\zeta^{219}x^{10}+x^3$	new	48506	936	$2^9\cdot 3\cdot 7$
$i=1$	$\zeta^{365}x^{129}+\zeta^{292}x^{66}+\zeta^{365}x^{17}+\zeta^{73}x^{10}+x^3$	new	48610	938	$2^9\cdot 3\cdot 7$
$i=1$	$\zeta^{365}x^{129}+\zeta^{365}x^{66}+\zeta^{146}x^{17}+\zeta^{365}x^{10}+x^3$	new	48612	938	$2^9\cdot 3\cdot 7$
$i=1$	$\zeta^{365}x^{129}+\zeta^{219}x^{66}+\zeta^{292}x^{17}+\zeta^{73}x^{10}+x^3$	new	48548	928	$2^9\cdot 3\cdot 7$
$i=1$	$\zeta^{73}x^{129}+\zeta^{365}x^{66}+\zeta^{73}x^{17}+\zeta^{73}x^{10}+x^3$	new	48548	928	$2^9\cdot 3\cdot 7$
$i=1$	$\zeta^{365}x^{129}+\zeta^{438}x^{66}+\zeta^{292}x^{10}+x^3$	new	48506	936	$2^9\cdot 3\cdot 7$
$i=1$	$\zeta^{365}x^{129}+x^{66}+\zeta^{438}x^{10}+x^3$	new	48604	928	$2^9\cdot 3\cdot 7$
$i=1$	$\zeta^{73}x^{129}+\zeta^{292}x^{66}+x^{10}+x^3$	new	48564	942	$2^9\cdot 3\cdot 7$
$i=1$	$\zeta^{73}x^{129}+x^{66}+\zeta^{219}x^{17}+x^3$	new	48604	928	$2^9\cdot 3\cdot 7$
$i=2$	$\zeta^{146}x^{257}+\zeta^{438}x^{68}+\zeta^{438}x^{12}+x^5$	new	48546	938	$2^9\cdot 3\cdot 7$
$i=2$	$\zeta^{146}x^{257}+\zeta^{365}x^{33}+\zeta^{365}x^{12}+x^5$	eq. to 8.1	48608	938	$2^9\cdot 3\cdot 7$
$i=2$	$\zeta^{73}x^{257}+\zeta^{146}x^{68}+x^{33}+x^5$	new	48564	942	$2^9\cdot 3\cdot 7$
$i=2$	$\zeta^{365}x^{257}+\zeta^{438}x^{68}+\zeta^{365}x^{33}+\zeta^{438}x^{12}+x^5$	new	48594	944	$2^9\cdot 3\cdot 7$
$i=2$	$\zeta^{146}x^{257}+\zeta^{219}x^{68}+\zeta^{73}x^{33}+x^{12}+x^5$	new	48520	932	$2^9\cdot 3\cdot 7$
$i=2$	$\zeta^{73}x^{257}+\zeta^{219}x^{68}+\zeta^{365}x^{33}+x^5$	new	48602	938	$2^9\cdot 3\cdot 7$
$i=4$	$\zeta^{292}x^3+\zeta^{146}x^{80}+\zeta^{73}x^{24}+x^{17}$	new	48520	932	$2^9\cdot 3\cdot 7$

cannot obtain APN functions by shifting F with a polynomial whose coefficients belong to $\mathbb{F}_2$.

Proposition 3.8. *For two integers k and m let $n=km$ and $q=2^k$. Consider a function $F\in\mathbb{F}_{2^n}[x]$ of the form*

$$F(x)=\sum_{i<j}b_{ij}x^{q^i+q^j}+\sum_i b_i x^{q^i}+c,$$

If $\mathbb{F}_4\subseteq\mathbb{F}_{2^n}$ or $k>1$, then any isotopic shift F_L with $L\in\mathbb{F}_{2^k}[x]$ cannot be APN. In particular, this holds for any quadratic function $F\in\mathbb{F}_{2^n}[x]$ with n even and $L\in\mathbb{F}_2[x]$.

Proof. For F and L as outlined, we have

$$F_L(x)=\sum_{i<j}b_{ij}[x^{q^i}L(x)^{q^j}+x^{q^j}L(x)^{q^i}]+c$$

and $L(x^q)=L(x)^q$. Note that for any $x\in\mathbb{F}_{2^k}$, $F_L(x)=c$. For $a\in\mathbb{F}_{2^n}$, we set $\Delta_a(x)=F_L(x+a)+F_L(x)+F_L(a)$.

If $k>1$, then $\Delta_a(x)=c$ for all $x,a\in\mathbb{F}_{2^k}$, so that F_L is not APN. If $\mathbb{F}_4=\{0,1,\alpha,\alpha+1\}\subseteq\mathbb{F}_{2^n}$, then consider $\Delta_\alpha(x)$. Clearly $\Delta_\alpha(0)=c$, while it is easily observed that $\Delta_\alpha(\alpha+1)=\Delta_\alpha(1)$. We have

$$\begin{aligned}\Delta_\alpha(\alpha+1)=&F_L(\alpha+1)+F_L(\alpha)+c\\ =&c+\sum_{i<j}b_{ij}[L(\alpha+1)^{q^i}(\alpha+1)^{q^j}+(\alpha+1)^{q^i}L(\alpha+1)^{q^j}\\ &+L(\alpha)^{q^i}\alpha^{q^j}+\alpha^{q^i}L(\alpha)^{q^j}]\\ =&c+\sum_{i<j}b_{ij}[L(\alpha+1)(\alpha+1)^{q^{j-i}}+(\alpha+1)L(\alpha+1)^{q^{j-i}}\\ &+L(\alpha)\alpha^{q^{j-i}}+\alpha L(\alpha)^{q^{j-i}}]^{q^i}.\end{aligned}$$

When $j-i$ is odd and $\mathbb{F}_4 \not\subseteq \mathbb{F}_{2^k}$, the term in the sum is zero as $\alpha^{q^{j-i}} = \alpha^2 = \alpha+1$, $L(\alpha)^{q^{j-i}} = L(\alpha+1)$ and $L(\alpha+1)^{q^{j-i}} = L(\alpha)$. If $j-i$ even or $\mathbb{F}_4 \subseteq \mathbb{F}_{2^k}$, then the term in the sum is again zero due to the fact that $\alpha^{q^{j-i}} = \alpha$ and $L(\alpha)^{q^{j-i}} = L(\alpha)$. In either case, we have $\Delta_\alpha(x) = c$ for $x = 0, 1, \alpha+1$, so F_L is not APN. □

3.5.1. Nonlinear shift for the Gold functions

If we consider an isotopic shift of a Gold function without the restriction that $L(x)$ is a linear function, then $L(x) = \sum_{j=0}^{2^n-1} c_j x^j$ and the isotopic shift will be of the form

$$\mathcal{G}_{i,L}(x) = x^{2^i} L(x) + xL(x)^{2^i}. \tag{4}$$

We have $\mathcal{G}_{i,L}(x^2)^{2^{-1}} = x^{2^i} M(x) + xM(x)^{2^i}$, where $M(x) = \sum c_j^{2^{-1}} x^j$, and also $\zeta^{-2^i-1}\mathcal{G}_{i,L}(\zeta x) = x^{2^i} N(x) + xN(x)^{2^i}$, where $N(x) = \sum c_j \zeta^{j-1} x^j$. Hence we obtain the following.

Proposition 3.9. *Let $\mathbb{F}_{2^n}^\star = \langle\zeta\rangle$. Assume that $\mathcal{G}_{i,L}$ is constructed with $L(x) = \sum_{j=0}^{2^n-1} c_j x^j$. Then, for any integers k, t, we have that $\mathcal{G}_{i,L}$ is linear equivalent to $\mathcal{G}_{i,M}$, where $M(x) = \sum_{j=0}^{2^n-1} (c_j \zeta^{k(j-1)})^{2^t} x^j$.*

As for the linear shifts, it is possible to restrict the search of one possible non-zero coefficient of the function.

In the following table we recall the list of known APN power maps (the list was conjectured to be complete in [11]).

Table 4: Known APN power functions x^d over $\mathbb{F}_{2^n}$

Functions	Exponents d	Conditions	Degree	Proven
Gold	2^i+1	$\gcd(i,n)=1$	2	[15, 18]
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n)=1$	$i+1$	[16, 17]
Welch	2^t+3	$n=2t+1$	3	[10]
Niho	$2^t+2^{\frac{t}{2}}-1$, t even $2^t+2^{\frac{3t+1}{2}}-1$, t odd	$n=2t+1$	$\frac{t+2}{2}$ $t+1$	[11]
Inverse	$2^{2t}-1$	$n=2t+1$	$n-1$	[2, 18]
Dobbertin	$2^{4i}+2^{3i}+2^{2i}+2^i-1$	$n=5i$	$i+3$	[12]

In odd dimension it is possible to obtain all power APN functions, except the Dobbertin functions, as the isotopic shifts of a Gold function by a monomial.

Theorem 3.10. *Over $\mathbb{F}_{2^n}$ with n an odd integer, let F be any known APN power function outside the class of Dobbertin functions. Then there exists a monomial $L(x) = ax^d$ and a Gold function $\mathcal{G}_i = x^{2^i+1}$ such that the shift $\mathcal{G}_{i,L}$ is EA-equivalent to F.*

Proof. As shown in Table 4, excluding the Dobbertin function, the known APN power functions are the Gold functions, the Kasami functions, the Welch function, the Niho functions and the inverse function. In the following we will show that it is possible for any of the mentioned functions, to construct an isotopic shift of a Gold function that is EA-equivalent to it.

1. Consider the Kasami function $x^{2^{2t}-2^t+1}$. If t is odd, then let i be an integer such that $n = 2i + t$. Then, considering $L = ax^{2^{n-i}+2^{n-i+1}...+2^{n-i+t-1}}$ we have
$$\begin{aligned}\mathcal{G}_{i,L} &= a^{2^i}x^{2^t} + ax^{2^{n-i}+2^{n-i+1}...+2^{n-i+t-1}+2^i} \\ &= a^{2^i}x^{2^t} + ax^{2^i(2^t+2^{t+1}...+2^{2t-1}+1)} \\ &= a^{2^i}x^{2^t} + ax^{2^i(2^{2t}-2^t+1)}.\end{aligned}$$
If t is even, let i be an integer such that $t = 2i$. Then, with $L = ax^{2^i+2^{i+1}+...+2^{3i-1}}$ we have $\mathcal{G}_{i,L} = a^{2^i}x^{2^{2t}-2^t+1} + ax^{2^{3i}}$.
2. For the inverse function, x^{2^n-2}, considering $L(x) = ax^{2^{2t}-2}$, where t is such that $n = 2t + 1$, we have $\mathcal{G}_{1,L} = a^2x^{2(2^n-2)} + ax^{2^{2t}}$.
3. Let $n = 2t + 1$ and consider the Welch function x^{2^t+3}. If t is odd, then consider i such that $t = 2i - 1$. With $L(x) = ax^{2^i+2^{i+1}}$ we obtain $\mathcal{G}_{i,L} = a^{2^i}x^{2^{2i}(2^{2i-1}+3)} + ax^{2^{i+2}}$. If t is even, then consider i such that $t = 2i$. Using $L(x) = ax^{2^{3i+1}+2^{3i+2}}$ we obtain $\mathcal{G}_{i,L} = a^{2^i}x^4 + ax^{2^{3i+1}(2^{2i}+3)}$.
4. For $n = 2t + 1$, with t odd, let $t = 2i - 1$. Then, with $L = ax^{2^n-2^i}$ we obtain that
$$\begin{aligned}\mathcal{G}_{i,L} &= a^{2^i}x^{2^i-2^{2i}+1} + ax = a^{2^i}x^{2^{2i}(2^{-i}+2^{-2i}-1)} + ax \\ &= a^{2^i}x^{2^{2i}(2^{3i-1}+2^{2i-1}-1)} + ax = a^{2^i}x^{2^{2i}(2^{(3t+1)/2}+2^t-1)} + ax\end{aligned}$$
is equivalent to the Niho function (indeed $(3t + 1)/2 = (6i - 3 + 1)/2 = 3i - 1$). If t is even, let $t = 2i$. Then with $L = ax^{2^{n-i}+2^{n-i+1}...+2^{n-1}}$
$$\begin{aligned}\mathcal{G}_{i,L} = &\quad a^{2^i}x^{2^i} + ax^{2^{n-i}+2^{n-i+1}...+2^{n-1}+2^i} \\ = &\quad a^{2^i}x^{2^i} + ax^{2^{n-i}(1+2...+2^{i-1}+2^{2i})} \\ = &\quad a^{2^i}x^{2^i} + ax^{2^{n-i}(2^i-1+2^{2i})}\end{aligned}$$
is equivalent to the Niho function.
5. Let $n = 2i + 1$ and j be an integer such that $\gcd(n, j) = 1$. Then with $L = ax^{2^{i+j}-2^i}$
$$\begin{aligned}\mathcal{G}_{i,L} &= a^{2^i}x^{2^{2i+j}-2^{2i}+1} + ax^{2^{i+j}} = a^{2^i}x^{2^{2i}(2^j+2^{-2i}-1)} + ax^{2^{i+j}} \\ &= a^{2^i}x^{2^{2i}(2^j+1)} + ax^{2^{i+j}}\end{aligned}$$
is equivalent to the Gold function with parameter j.

□

Remark 3.11. *From computational results, for n even, it seems that it is not possible to obtain APN functions as the isotopic shifts of a Gold map by (non-linear) monomials. The search has been performed for $n = 4, 6, 8, 10$, considering also non-APN Gold exponents.*

Problem 3.12. *Is it possible to obtain the Dobbertin function as an isotopic shift of a Gold function by a non-linear L?*

Problem 3.13. *Is it possible to obtain the same result for n an even integer and L a non-linear multinomial?*

4. Conclusions

Starting from the work [5], we introduced some generalizations of the isotopic shift construction for the case when the starting function is a Gold power function. In particular, using a generalized form of the isotopic shift with $\mathbb{F}_{2^m}$-polynomials, we were able to construct a general family of quadratic APN functions. This allowed us to classify into a family some of the previously known unclassified examples of APN functions for $n = 8, 9$, and to provide new APN functions on $\mathbb{F}_{2^8}$ and $\mathbb{F}_{2^9}$. The computations performed were restricted to linear maps with coefficients in the subfield. We expect that, without such restriction, it is possible to find additional new APN functions.

We also investigated the case of constructing an isotopic shift with a nonlinear function. In this case, for any odd n, we can obtain all known power APN functions (except the Dobbertin ones) using a nonlinear monomial function.

Acknowledgements

The research of this paper was supported by Trond Mohn Foundation.

References

[1] A.A. Albert, *Finite division algebras and finite planes*, Combinatorial Analysis: Proceedings of the 10th Symposium in Applied Mathematics (Providence), Symposia in Applied Mathematics, vol. 10, American Mathematical Society, 1960, pp. 53–70.

[2] T. Beth, C. Ding, *On almost perfect nonlinear permutations*, Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Science, 765, Springer-Verlag, New York, 1993, pp. 65-76.

[3] E. Biham, A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, J. Cryptol., vol. 4, no. 1, pp. 3-72, 1991.

[4] K. A. Browning, J.F. Dillon, R.E. Kibler, and M. T. McQuistan. *APN Polynomials and Related Codes*. J. of Combinatorics, Information and System Sciences, 34(1-4):135-159, 2009

[5] L. Budaghyan, M. Calderini, C. Carlet, R. Coulter, I. Villa, *Constructing APN functions through isotopic shifts*. To appear in IEEE Trans. Inform. Theory. Preliminary version in IACR ePrint Archive: Report 2018/769.

[6] L. Budaghyan, M. Calderini, C. Carlet, R. Coulter and I. Villa, *On Isotopic Shift Construction for Planar Functions*, 2019 IEEE International Symposium on Information Theory (ISIT), Paris, France, 2019, pp. 2962-2966.

[7] L. Budaghyan, M. Calderini, I. Villa, *On relations between CCZ- and EA-equivalences*. Cryptogr. Commun. `https://doi.org/10.1007/s12095-019-00367-5`(2019).

[8] L. Budaghyan, C. Carlet, G. Leander, *Constructing New APN Functions from Known Ones*, Finite Fields and Their Applications, **15** (2009), pp. 150–159

[9] L. Budaghyan, C. Carlet, G. Leander, *On a Construction of Quadratic APN Functions.*, Proceedings of IEEE Information Theory workshop ITW'09, Oct. 2009, pp. 374–378 .

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

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

[12] H. Dobbertin, *Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5*, Proceedings of Finite Fields and Applications FQ5, 2000, pp. 113-121.

[13] E. Edel, A. Pott, *A new almost perfect nonlinear function which is not quadratic*, Adv. Math. Commun. **3** (2009), 59–81.

[14] F. Göloğlu and J. Pavlu, Search for APN permutations among known APN functions. Presented at BFA2019.

[15] R. Gold, *Maximal recursive sequences with 3-valued recursive cross-correlation functions*, IEEE Trans. Inform. Theory, 14, 1968, pp. 154-156.

[16] H Janwa, R. Wilson, *Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cycle codes*, Proceedings of AAECC-10, LNCS, vol. 673, Berlin, Springer-Verlag, 1993, pp. 180-194.

[17] T. Kasami, *The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes*, Inform. and Control, 18, 1971, pp. 369-394.

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

[19] S. Yoshiara, *Equivalences of quadratic APN functions.* Journal of Algebraic Combinatorics 35.3 (2012): 461-475.

[20] Y. Yu, M. Wang, and Y. Li, *A matrix approach for constructing quadratic APN functions*, Designs, codes and cryptography 73.2 (2014): 587-600.