On Quadratic Almost Perfect Nonlinear Functions and Their Related Algebraic Object

Guobian Weng, Yin Tan, and Guang Gong

School of Mathematical Sciences, Dalian University of Technology, Liaoning 116024, China
gbweng@dlut.edu.cn
Department of Electrical and Computer Engineering, University of Waterloo
Waterloo, Ontario, Canada
{y24tan, ggong}@uwaterloo.ca

Abstract. It is well known that almost perfect nonlinear (APN) functions achieve the lowest possible differential uniformity for functions defined on fields with even characteristic, and hence, from this point of view, they are the most ideal choices for S-boxes in block and stream ciphers to avoid differential attack. They are also interesting by the link to many other areas, for instance topics in coding theory and combinatorics. In this paper, we present a characterization of quadratic APN functions by a certain kind of algebraic object, which is called an APN algebra in this paper. By this characterization and with the help of a computer, we discover 285 new (up to CCZ equivalence) quadratic APN functions on $\mathbb{F}_{2^7}$, and 10 new quadratic APN functions on $\mathbb{F}_{2^8}$. This is a remarkable contrast to the currently known 17 APN functions on $\mathbb{F}_{2^7}$, and 23 such functions on $\mathbb{F}_{2^8}$. After studying some properties of these newly obtained functions, some open problems are proposed based on the computational results.

Keywords: Almost perfect nonlinear functions, Quadratic function, Substitution box, Algebra

1 Introduction

In the modern design of block and stream ciphers, functions defined on finite fields are chosen as Substitution boxes (or S-box in short) to bring the confusion to the cipher. The S-box needs to be designed carefully to avoid many attacks on the cipher. For instance, the S-boxes are required to be with low differential uniformity (defined below) to prevent the differential cryptanalysis proposed by Biham and Shamir [1].

It is well-known that almost perfect nonlinear (or APN in short, see definition in Section 2) functions achieve the lowest possible differential uniformity for functions de-

fined on fields with even characteristic, and therefore, from this point of view, they are the most ideal choices for S-boxes. Such functions are not only interesting in the cryptography, they are demonstrated to be linked with many other topics in the theory of sequences [16], difference sets, bent functions [20] and finite geometry [15].

APN functions were firstly introduced by Nyberg in [18], and several such functions were constructed in her paper. Since then, many power APN functions are discovered by various researchers, see Table 1 for a list of all known power APN functions. It is conjectured that the list of power APN functions is complete (up to CCZ-equivalence, see the definition in Section 2).

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

	Exponent d	Conditions
Gold	2^i+1	$\gcd(i,n)=1$
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n)=1$
Welch	2^t+3	$n=2t+1$
Niho	$2^t+2^{t/2}-1$, t even $2^t+2^{(3t+1)/2}-1$, t odd	$n=2t+1$
Inverse	2^n-2	$n=2t+1$
Dobbertin	$2^{4t}+2^{3t}+2^{2t}+2^t-1$	$n=5t$

Besides the preceding power APN functions, in [12], two sporadic binomial APN functions defined on $\mathbb{F}_{2^{10}}$: $x^3+\omega x^{36}$, where ω has order 3 or 93; and $x^3+\omega x^{36}$, where ω has order 273 or 585 are discovered. These two examples are verified to be CCZ-inequivalent to any power functions in Table 1. They were soon generalized into infinite families in [4]. In 2006, Dillon gave more sporadic APN polynomials on $\mathbb{F}_{2^6}$ which are not CCZ-equivalent to any power functions in his talk [10]. These sporadic examples became a source of obtaining new infinite families of APN functions. Many new infinite families are successfully discovered in the sequel, see [2, 3, 6, 7] and the references therein. We should note that all infinite families of APN functions constructed since 2005 are quadratic ones (see definition in Section 2).

Besides the above method of obtaining new infinite families by generalizing sporadic examples, in [5], the switching method was introduced to construct new APN functions, and the APN function $x^3+\mathrm{Tr}(x^9)$ was found. This function is beautiful in the sense that it is obtained via changing one component function of a known APN function x^3. The switching method was further explored in [13] and more sporadic APN functions were discovered. More precisely, they discovered one new APN function on $\mathbb{F}_{2^6}$, one new on $\mathbb{F}_{2^7}$ and eleven ones on $\mathbb{F}_{2^8}$. At this stage, due to the discovery of many quadratic APN functions, the following question was proposed in [13]:

Problem 1. Does the number of CCZ inequivalent APN functions on $\mathbb{F}_{2^n}$ grows exponentially with the increase of n?

It is conjectured that the above problem has a positive answer, but the number of known quadratic APN functions so far cannot give a strong evidence of this conjecture. One may refer to Table 2 for the number of APN functions on small fields known so far.

We should note that, comparing to the discovery of many quadratic APN functions, few non-quadratic ones are known. Actually, except the power APN functions, there is no single infinite families of nonquadratic APN functions is known (a sporadic example on $\mathbb{F}_{2^6}$ was found in [13]). Also, there is little knowledge about the existence of APN permutations on fields with even degrees, i.e. $\mathbb{F}_{2^{2k}}$. Until now, there is only one such function on $\mathbb{F}_{2^6}$ which was found by Dillon in [11]. This APN permutation is CCZ-equivalent to the quadratic APN function $x^3+x^{10}+ux^{24}$ on $\mathbb{F}_{2^6}$, where u is a primitive element of $\mathbb{F}_{2^6}$. To discover more APN permutations on $\mathbb{F}_{2^{2k}}$ is called the *BIG APN Problem*. By Dillon's method, finding more quadratic APN functions may give a hope to obtain APN permutations on $\mathbb{F}_{2^{2k}}$.

In this paper, we present a new characterization of quadratic APN functions. It is shown that such functions are conceptually equivalent to certain algebraic object, which is called an APN algebra in this paper. More precisely, let $\mathfrak{A}=(\mathbb{F}_{2^n},+,*)$, where $+$ is the finite field addition and $*$ is a well defined binary operation on $\mathbb{F}_{2^n}$. We call $\mathfrak{A}$ an *APN algebra* if the operation $*$ satisfies the commutative and distributive law, and $x*y=0$ if and only if $x=y$ or one of x,y is 0 (also defined in Section 3). Now, for a function

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, Theorem 1 in Section 3 shows that if F is a quadratic APN function, $\mathfrak{A} = (\mathbb{F}_2^n, +, *)$ is an APN algebra, where

$$x * y = F(x) + F(y) + F(x + y) + F(0).$$

Conversely, for any APN algebra $\mathfrak{A} = (\mathbb{F}_2^n, +, *)$, a quadratic APN function can be defined through it (see (6) in Section 3). This characterization enables us to give a unifying treatment of quadratic APN functions in terms of APN algebras.

Furthermore, in Section 3, we present a matrix representation of the APN algebra, which is very useful when search for new APN functions on small fields. Surprisingly, by a computer, many new quadratic APN functions on small fields are discovered. We use the following table to compare the number of APN functions known so far (c.f. [13]) and newly discovered in this paper on $\mathbb{F}_{2^6}, \mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$.

Table 2. Number of APN functions on $\mathbb{F}_{2^n}$ in [13] and in this paper

n	♯ of APN in [13]	♯ of newly found APN in this paper
6	14	0
7	17	≥ 285
8	23	10

Several remarks on Table 2 are in the sequel. Firstly, with the help of a computer, we have a proof that only 13 quadratic APN functions on $\mathbb{F}_{2^6}$. We should mention that this fact is also known by Yves Edel and Philippe Langevin. Secondly, on $\mathbb{F}_{2^7}$, we found $30,000$ quadratic APN functions by a personal computer in two days. We randomly choose $5,000$ of them to test their newness, and find 285 new functions. It is reasonably believe that more new functions may be found amongst the remaining $25,000$ functions. Finally, on $\mathbb{F}_{2^8}$, we test 500 quadratic APN functions, and 10 new ones are obtained. It is not the purpose of this paper to break a record of the number of new APN functions, but providing mathematical characterization and exploring properties of quadratic APN functions. All these computations are done by a personal laptop, it is very possible that more APN functions may be found by a more powerful computer.

The rest of the paper is organized as follows. In Section 2, we give necessary definitions and results used later. The relationship between APN algebras and quadratic APN functions are discussed in Section 3. We also describe the matrix representation of APN algebras and construct an APN algebra there. Section 4 is devoted to explaining two techniques we used to search for new quadratic APN functions on small fields using the above characterization. Some of the newly found quadratic APN functions on $\mathbb{F}_{2^7}, \mathbb{F}_{2^8}$ are presented in this Section as well. We discuss some properties of these functions in Section 5, and propose some open problems which are based on the computational result. Finally, we give some concluding remarks in Section 6.

2 Preliminaries

In this Section, we give the definitions and results which will be used in the following sections.

2.1 Differential and Walsh spectrum

Let $\mathbb{F}_{2^n}$ be a finite field and $\mathbb{F}_{2^n} = \mathbb{F}_{2^n} \setminus \{0\}$. Let F be a function F on $\mathbb{F}_{2^n}$, for any two-tuple $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$, define

$$\delta_F(a, b) = \sharp\{x : x \in \mathbb{F}_{2^n} | F(x + a) + F(x) = b\},$$

where $\sharp S$ denotes the cardinality for a set S. The value

$$\Delta_F \triangleq \max_{(a,b)\in\mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}} \delta_F(a, b)$$

is called the *differential uniformity* of F, or call F a *differentially Δ_F-uniform* function. The multiset $\{\delta_F(a, b) : (a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}\}$ is called the *differential spectrum* of F. In particular, we call F *almost perfect nonlinear* (APN) if $\Delta_F = 2$.

Another common approach to characterize the nonlinearity of F is as follows. For the function F, the *Walsh (Fourier) transform* $F^{\mathcal{W}} : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{C}$ of F is defined by:

$$F^{\mathcal{W}}(a, b) := \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(aF(x)+bx)}, \tag{1}$$

where $\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{2^i}$ denotes the absolute trace function. The multiset $\mathcal{W}_F := \{F^{\mathcal{W}}(a,b) : a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}\}$ is called the *Walsh spectrum* of F. Some researchers call the multiset containing the Walsh spectrum and its negative the *extended Walsh spectrum* of F. Furthermore, it is conjectured that $\max|\mathcal{W}_F(a,b)| \geq 2^{(n+1)/2}$ when n is odd, and it is known $\max|\mathcal{W}_F(a,b)| \geq 2^{n/2+1}$ when n is even. We call F an *almost bent* (AB) function if $F^{\mathcal{W}}(a,b) \in \{0, \pm 2^{(n+1)/2}\}$ for all $a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}$. Obviously, AB functions can only exist on $\mathbb{F}_{2^n}$ with n odd. It is well known that any AB function is an APN function ([9]), but not vice versa ([13]). However, any quadratic APN function on $\mathbb{F}_{2^n}$ with n odd must be an AB function ([8]).

Finally, a function F is called *quadratic* if for all $a \in \mathbb{F}_{2^n}^*$, the function

$$L_a(x) \triangleq F(x+a) + F(x) + F(a)$$

is linear.

2.2 EA and CCZ equivalence

Two functions F and G defined on $\mathbb{F}_{2^n}$ are called *extended affine* (EA-) equivalent if there exist affine permutations $A_1, A_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and an affine function A such that $G = A_1 \circ F \circ A_2 + A$. They are called *Carlet-Charpin-Zinoviev* (CCZ) equivalent if their graphs $\mathcal{G}_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ and $\mathcal{G}_G = \{(x, G(x)) : x \in \mathbb{F}_{2^n}\}$ are affine equivalent, that is, there exists an affine automorphism L of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $L(\mathcal{G}_F) = \mathcal{G}_G$. It is well known that EA equivalence implies CCZ equivalence, but not vise versa. However, for two quadratic APN functions F, G, it is recently shown in [21] that they are CCZ equivalent if and only if they are EA equivalent.

Usually, it is difficult to judge the CCZ equivalence of two APN functions. In [13], a coding theory method to characterize the CCZ equivalence is given. First note that throughout this paper, we always use the identification of the additive group of the vector space $\mathbb{F}_2^n$ with the additive group of the finite field $\mathbb{F}_{2^n}$. More precisely, let $\{\alpha_1, \cdots, \alpha_n\}$ be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, for each element $x \in \mathbb{F}_{2^n}$, there exist a unique vector $\mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{F}_2^n$ such that $x = x_1\alpha_1 + \cdots + x_n\alpha_n$. We use the notation $\mathbf{x}$ to denote the corresponding vector in $\mathbb{F}_2^n$ of the element $x \in \mathbb{F}_{2^n}$.

Let F be an APN function, define the matrix $C_F \in \mathbb{F}_2^{(2n+1)\times 2^n}$ as follows:

$$C_F = \begin{bmatrix} \cdots & 1 & \cdots \\ \cdots & \mathbf{x} & \cdots \\ \cdots & \mathbf{F(x)} & \cdots \end{bmatrix},$$

where the columns of C_F are ordered with respect to some ordering of the elements of $\mathbb{F}_{2^n}$ (in the matrix the elements $\mathbf{x}, \mathbf{F(x)}$ are regarded as elements in $\mathbb{F}_2^n$ as explained above). Let $\mathcal{C}_F$ be the linear code generated by C_F. We have the following result.

Result 1 *[13] Let F, G be two APN functions and $\mathcal{C}_F, \mathcal{C}_G$ be the linear codes generated from them as above. Then F and G are CCZ equivalent if and only if $\mathcal{C}_F$ and $\mathcal{C}_G$ are equivalent.*

There are some invariants of APN functions under CCZ-equivalence. For instance, the differential spectrum and extended Walsh spectrum of APN functions. Note that the same value of these invariants are only the necessary condition of two functions being CCZ-equivalent, but they may imply some properties of APN functions, see Result 2 for instance. For the convenience of the discussion in Section 5, we review some invariants developed in [13].

Using the language of group rings, an APN function F can be denoted by $G_F = \sum_{x\in\mathbb{F}_{2^n}}(x, F(x))$. It is not hard to see that F is APN if and only if

$$G_F \cdot G_F = 2^n \cdot (0,0) + 2 \cdot D_F \tag{2}$$

for some $D_F \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \setminus \{(0,0)\}$. Denoting by $Dev(G_F)$ and $Dev(D_F)$ the two developments (see definition in [13]) of G_F and D_F. By [13], if F and G are CCZ equivalent, the designs $Dev(G_F)$ and $Dev(D_F)$ are isomorphic. Therefore, the order of automorphism groups and the 2-rank of their incidence matrices (which are denoted by Γ- and Δ-rank respectively) are invariant under CCZ equivalence. Moreover, let $\mathcal{M}(G_F)$ (resp. $\mathcal{M}(D_F)$) be the set of automorphisms of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $\sigma(G_F) = G_F \cdot (u, v)$ (resp. $\sigma(D_F) = D_F \cdot (u, v)$) for some $(u, v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$. It is shown in [13] that $\mathcal{M}(G_F)$ and $\mathcal{M}(D_F)$ are groups under the multiplication of $\mathrm{Aut}(\mathbb{F}_{2^n} \times \mathbb{F}_{2^n})$, which are called *multiplier groups* and are also invariant under CCZ equivalence.

These parameters are interesting as they imply some properties of the APN function.

Result 2 *[14] Let F be an APN function on $\mathbb{F}_{2^n}$ and $v = \sharp\mathcal{M}(G_F)$. Then: (1) $n\cdot(2^n-1) \mid v$ if F is CCZ equivalent to a power mapping; and (2) $n \mid v$ if F is CCZ equivalent to a polynomial in $\mathbb{F}_2[x]$.*

We should mention that one reason for us to introduce the above invariants is that they can be easily computed by MAGMA, which helps us study the newly obtained APN functions.

3 Quadratic APN functions and APN algebras

In this Section, we will establish a relationship between quadratic APN functions and APN algebras. We first introduce a matrix representation of an APN algebra and then use it to prove the aforementioned relationship. This representation is very useful to search for new quadratic APN functions on small fields, which is discussed in Section 4. First, we give the definition of the APN algebra.

Definition 1. *Let $\mathbb{F}_{2^n}$ be a finite field and $\mathfrak{A} = (\mathbb{F}_{2^n}, +, *)$, where $+$ is the finite field addition and $*$ is a well defined binary operation on $\mathbb{F}_{2^n}$. $\mathfrak{A}$ is called APN algebra if the operation $*$ satisfies the commutative and distributive law, and $x * y = 0$ if and only if $x = y$ or one of x, y is 0.*

3.1 Matrix representation of APN algebra

Define an $n \times n$ matrix A by

$$A = (a_{ij})_{n\times n}\,,\ a_{ij} = \alpha_i * \alpha_j. \tag{3}$$

Note that, by the definition of APN algebra, $a_{ii} = 0$ for all $1 \le i \le n$ and $A^{\mathrm{T}} = A$. Now, we may use the matrix A to represent the APN algebra $\mathfrak{A}$ by the following result.

Proposition 1. *Let $\mathfrak{A} = (\mathbb{F}_{2^n}, +, *)$ be an APN algebra and A be the its corresponding matrix defined in (3). For any elements $x, y \in \mathbb{F}_{2^n}$, we have $x * y = \mathbf{x}A\mathbf{y}^{\mathrm{T}}$, where $\mathbf{x}, \mathbf{y}$ are the corresponding vectors of x, y in $\mathbb{F}_2^n$.*

Proof. Let $\mathbf{x} = (x_1, \cdots, x_n)$ and $\mathbf{y} = (y_1, \cdots, y_n)$. We have

$$\begin{aligned} x * y &= \left(\sum_{i=1}^{n} x_i\alpha_i\right) * \left(\sum_{i=1}^{n} y_i\alpha_i\right) \\ &= \sum_{i,j=1}^{n} x_i y_j \left(\alpha_i * \alpha_j\right) \\ &= \mathbf{x} A \mathbf{y}^{\mathrm{T}}. \end{aligned}$$

We finish the proof. □

The next result gives a property of the matrix A, which is used in Section 4 to search for new APN functions on small fields.

Proposition 2. *Let $\mathfrak{A} = (\mathbb{F}_{2^n}, +, *)$ be an APN algebra and A be the matrix defined in (3). Then for each row (column) of A, the $n-1$ nonzero elements are linearly independent over $\mathbb{F}_2$.*

Proof. Since A is symmetric, we only prove the result is true for each row. Without loss of generality, we prove the $n-1$ nonzero elements $a_{12}, \cdots, a_{1n}$ in the first row of A are linear independent. Assume there exists $(t_2, \cdots, t_n) \in \mathbb{F}_2^{n-1}$ such that $t_2 a_{12} + \cdots + t_n a_{1n} = 0$. Substituting $a_{ij} = \alpha_i * \alpha_j$ we have

$$\begin{aligned} 0 &= t_2\alpha_1 * \alpha_2 + \cdots + t_n\alpha_1 * \alpha_n \\ &= \alpha_1 * (t_2\alpha_2 + \cdots + t_n\alpha_n). \end{aligned}$$

Then, by the definition of APN algebra, we have $t_2\alpha_2 + \cdots + t_n\alpha_n$ equals 0 or α_1. Clearly $t_2\alpha_2 + \cdots + t_n\alpha_n \neq \alpha_1$ as $\{\alpha_1, \cdots, \alpha_n\}$ is a basis. Similarly, $t_2\alpha_2 + \cdots + t_n\alpha_n = 0$ if and only if $t_i = 0$ for $2 \leq i \leq n$, which implies that $\alpha_2, \cdots, \alpha_n$ is linear independent. □

Furthermore, for simplicity, we write the matrix A as in the form $A = B + B^{\mathrm{T}}$, where

$$B = \begin{pmatrix} 0 & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & 0 & a_{23} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix}_{n\times n}. \tag{4}$$

3.2 The relationship

Now we are ready to give the main result of this section.

Theorem 1. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a quadratic APN function. Define the multiplication $*_F : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ by*

$$x *_F y = F(x + y) + F(x) + F(y) + F(0). \tag{5}$$

Then $(\mathbb{F}_{2^n}, +, *_F)$ is an APN algebra. Conversely, let $\mathfrak{A} = (\mathbb{F}_{2^n}, +, *)$ be an APN algebra. Let the matrices A, B be the ones defined in (3) and (4). Then the function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by

$$F(x) = \mathbf{x}B\mathbf{x}^{\mathrm{T}} \tag{6}$$

is a quadratic APN function. Moreover, $x *_F y = x * y$ for $x, y \in \mathbb{F}_{2^n}$.

Proof. First, for the quadratic APN function F, we show that $\mathfrak{A} = (\mathbb{F}_{2^n}, +, *_F)$ is an APN algebra, where $*_F$ is defined in (5). Clearly, for all $x, y, z \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned} x *_F y &= y *_F x && \text{(commutative law)},\\ x *_F (y + z) &= x *_F y + x *_F z && \text{(distributive law)}. \end{aligned}$$

Note that the distributive law is followed from $F(x + a) + F(x) + F(a) + F(0)$ is linear for any nonzero a as F is quadratic. It is also clear that $x *_F y = 0$ if and only if $x = y$ or one of x, y is 0. Indeed, assume that $x *_F y = F(x + y) + F(x) + F(y) + F(0) = 0$ and $y \neq 0$, we have $F(x + y) + F(x) = F(y) + F(0)$. It then follows from F is an APN function that $x = 0$ or $x = y$.

Conversely, for the APN algebra $\mathfrak{A} = (\mathbb{F}_{2^n}, +, *)$, we need to show the function F defined in (6) is a quadratic APN function. Obviously, F is quadratic. For any nonzero $a \in \mathbb{F}_{2^n}$, we need to demonstrate the equation

$$\Delta_a(x) = F(x + a) + F(x) + F(a) = 0 \tag{7}$$

has at most two solutions. Substituting F defined in (6) into (7) we get

$$\begin{aligned} 0 = \Delta_a(x) &= \mathbf{x}B\mathbf{a}^{\mathrm{T}} + \mathbf{a}B\mathbf{x}^{\mathrm{T}} = \mathbf{x}B\mathbf{a}^{\mathrm{T}} + (\mathbf{a}B\mathbf{x}^{\mathrm{T}})^{\mathrm{T}} \\ &= \mathbf{x}(B + B^{\mathrm{T}})\mathbf{a}^{\mathrm{T}} = \mathbf{x}A\mathbf{a}^{\mathrm{T}} \\ &= x * a. \end{aligned}$$

Since $\mathfrak{A}$ is an APN algebra, then from above we have $x = 0$ or a, which follows that F is an APN function. Finally, it is easy to verify that $x * y = x *_F y$ for all $x, y \in \mathbb{F}_{2^n}$. We finish the proof. □

Remark 1. Expanding the quadratic APN function in (6), we may write F as

$$F(x) = \sum_{\substack{i,j=1 \\ i<j}}^{n} x_i x_j(\alpha_i * \alpha_j),\ \mathbf{x} = (x_1, \cdots, x_n).$$

Two APN algebras $\mathfrak{A}_1 = (\mathbb{F}_{2^n}, +, *_1)$ and $\mathfrak{A}_2 = (\mathbb{F}_{2^n}, +, *_2)$ are said to be *isomorphic* if there exist two linear permutations L_1, L_2 such that

$$L_1(x) *_1 L_1(y) = L_2(x *_2 y)$$

for all $x, y \in \mathbb{F}_{2^n}$. The following result shows that two quadratic APN functions are EA equivalent (or equivalently, CCZ equivalent by [21]) if and only if their corresponding APN algebras are isomorphic.

Theorem 2. *Let F_1, F_2 be two quadratic APN functions on $\mathbb{F}_{2^n}$. If F_1 and F_2 are EA equivalent, their corresponding APN algebras $\mathfrak{A}_1 = (\mathbb{F}_{2^n}, +, *_{F_1})$ and $\mathfrak{A}_2 = (\mathbb{F}_{2^n}, +, *_{F_2})$ are isomorphic. Conversely, if two APN algebras $\mathfrak{A}_1 = (\mathbb{F}_{2^n}, +, *_1)$ and $\mathfrak{A}_2 = (\mathbb{F}_{2^n}, +, *_2)$ are isomorphic, their corresponding APN functions F_1, F_2 defined in (6) are EA equivalent.*

Proof. Suppose that F_1 and F_2 are EA-equivalent, then there exist affine permutations A_1, A_2 and an affine function A_3 such that

$$F_1 \circ A_1 + A_3 = A_2 \circ F_2 \tag{8}$$

Let $A_1(x) = L_1(x) + c_1$ and $A_2(x) = L_2(x) + c_2$, where L_1, L_2 are linear permutations. Substituting A_1, A_2 into (8), we may get

$$\begin{aligned} &F_1(A_1(x)) + F_1(A_1(y)) + F_1(A_1(x+y)) + F_1(A_1(0)) \\ &= L_2\left(F_2(x) + F_2(y) + F_2(x+y) + F_2(0)\right). \end{aligned}$$

Since F_1 is quadratic, the above equation may be simplified as

$$\begin{aligned} &F_1(L_1(x)) + F_1(L_1(y)) + F_1(L_1(x+y)) + F_1(L_1(0)) \\ &= L_2(F_2(x) + F_2(y) + F_2(x+y) + F_2(0)), \end{aligned}$$

which follows that $L_1(x) *_{F_1} L_1(y) = L_2(x *_{F_2} y)$ and hence $\mathfrak{A}_1, \mathfrak{A}_2$ are isomorphic.

Conversely, let $\mathfrak{A}_1, \mathfrak{A}_2$ be two isomorphic APN algebras and F_1, F_2 be their corresponding quadratic APN functions. To show that F_1, F_2 are EA equivalent, we need to demonstrate that there exist affine permutations A_1, A_2 such that $F_1 \circ A_1 + A_2 \circ F_2$ is affine. Since $\mathfrak{A}_1, \mathfrak{A}_2$ are isomorphic, there exist linear permutations L_1, L_2 such that

$$L_1(x) *_1 L_1(y) = L_2(x *_2 y).$$

By Theorem 1, we have

$$L_1(x) *_{F_1} L_1(y) = L_2(x *_{F_2} y).$$

Expanding the above equation we may see that $F_1 \circ L_1 + L_2 \circ F_2$ is affine. We finish the proof. □

3.3 A construction of APN algebra $(\mathbb{F}_{2^{2k}}, +, *)$

In the following, we give an example of APN algebra.

Theorem 3. *Let $\mathbb{F}_{2^n}$ be a finite field with $n = 2k$ and write $\mathbb{F}_{2^n} = \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$. Let s be an integer with $\gcd(s, n) = 1$. For any $x = (a, b), y = (c, d) \in \mathbb{F}_{2^n}$, define $x * y$ as*

$$x * y = \big(ad + bc, t_0(ac^{2^s} + a^{2^s}c) + t_1(a^{2^s}d + c^{2^s}b) + t_2(ad^{2^s} + cb^{2^s}) + t_3(b^{2^s}d + bd^{2^s})\big) \quad (9)$$

where the polynomial

$$t_0x^{2^s+1} + t_1x^{2^s} + t_2x + t_3 \in \mathbb{F}_{2^n}[x] \tag{10}$$

has no zeros over $\mathbb{F}_{2^k}$*. Then* $\mathfrak{A} = (\mathbb{F}_{2^n}, +, *)$ *is an APN algebra.*

Proof. The commutative and distributive law can be verified easily for $\mathfrak{A}$. It is also clear that $x * y = 0$ if $x = y$ or one of x, y is zero. Now, assume that $x * y = 0$, we need to show that either $x = y$ or one of x, y is 0. W.l.o.g. suppose $x \neq 0$, then

$$0 = ad + bc, \tag{11}$$

$$0 = t_0(ac^{2^s} + a^{2^s}c) + t_1(a^{2^s}d + c^{2^s}d) + t_2(ad^{2^s} + cb^{2^s}) + t_3(b^{2^s}d + bd^{2^s}). \tag{12}$$

By (11), the determinant

$$0 = \begin{vmatrix} a & c \\ b & d \end{vmatrix},$$

which follows that $c = ta, d = tb$ for some $t \in \mathbb{F}_{2^k}$. Substituting them in (12) we have

$$(t + t^{2^s})(t_0a^{2^s+1} + t_1a^{2^s}b + t_2ab^{2^s} + t_3b^{2^s+1}) = 0.$$

Dividing b^{2^s+1} across the above equation we obtain

$$(t + t^{2^s})\left(t_0\left(\frac{a}{b}\right)^{2^s+1} + t_1\left(\frac{a}{b}\right)^{2^s} + t_2\left(\frac{a}{b}\right)^{2^s} + t_3\right) = 0.$$

By the assumption that the polynomial $t_0x^{2^s+1} + t_1x^{2^s} + t_2x + t_3 = 0$ has no zero over $\mathbb{F}_{2^k}$, we can only have $t + t^{2^s} = 0$, which follows that $t \in \mathbb{F}_{2^{\gcd(s,n)}} = \mathbb{F}_2$. Now, from $c = ta, d = tb$, we have: $x = y$ when $t = 1$ and $y = 0$ when $t = 0$. We finish the proof. □

Remark 2. The existence of the polynomial of the form (10) with no zeros over $\mathbb{F}_{2^k}$ can be seen as follows. Firstly, it is clear that there exist t_0, t_1, t_2 such that the polynomial $t_0x^{2^s+1} + t_1x^{2^s} + t_2x$ is not a permutation of $\mathbb{F}_{2^k}$, then there must have an element t_3 such that the polynomial $t_0x^{2^s+1} + t_1x^{2^s} + t_2x + t_3$ have no zeros over $\mathbb{F}_{2^k}$ as otherwise it follows that $t_0x^{2^s+1} + t_1x^{2^s} + t_2x$ is a permutation, which is a contradiction.

Corollary 1. *Let $F : \mathbb{F}_{2^{2k}} \to \mathbb{F}_{2^{2k}}$ be the function defined by*

$$F(x) = \sum_{\substack{i,j=1 \\ i<j}}^{n} x_i x_j \left(\alpha_i * \alpha_j\right), \ \mathbf{x} = (x_1, \cdots, x_{2k}),$$

where the multiplication is defined in (9). Then F is a quadratic APN function.

By MAGMA, for small values, we verified the newness of the APN function in Corollary 1. It is found that, when k is even, F is equivalent to the multinomial one in [6, Theorem 1]; and when k is even, F is equivalent to the hexanomial one in [3, Theorem 3]. The following Table 3 lists the computational results of the APN function F. Recall that the notations of Γ-rank, Δ-rank, $Dev(G_F)$, $Dev(D_F)$ and $\mathcal{M}(G_F)$ are defined in Section 2.2. The symbol "$-$" means that our computer cannot calculate that parameter.

Table 3. Invariants of the APN functions in Corollary 1

n	Γ-rank	Δ-rank	$\sharp\mathrm{Aut}(Dev(G_F))$	$\sharp Aut(\mathrm{Dev}(D_F))$	$\sharp\mathcal{M}(G_F)$
6	1146	94	$2^{18} \cdot 3^2 \cdot 7$	$2^{19} \cdot 3^2 \cdot 7$	$2^6 \cdot 3^2 \cdot 7$
8	13200	414	$-$	$-$	$2^{10} \cdot 3^2 \cdot 5$
10	$-$	$-$	$-$	$-$	$2^{10} \cdot 3 \cdot 5 \cdot 31$

In general, we cannot prove the CCZ-equivalence of the APN functions from Corollary 1 to the ones in [6, Theorem 1] and in [3, Theorem 3], we left this as an open problem.

Problem 2. To show that, when k is odd, the APN functions in Corollary 1 is CCZ-equivalent to the one in [3, Theorem 3]; when k is even, they are CCZ-equivalent to the one in [6, Theorem 1].

4 Discovering new APN functions

By Theorem 1, finding a quadratic APN function F is equivalent to finding its corresponding APN algebra $\mathfrak{A}$. Furthermore, by Proposition 1, an APN algebra $\mathfrak{A}$ can be

represented as a matrix of the form

$$A = \begin{pmatrix} 0 & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{12} & 0 & a_{23} & \cdots & a_{2n} \\ a_{13} & a_{23} & 0 & \cdots & a_{3n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{1n} & a_{2n} & a_{3n} & \cdots & 0 \end{pmatrix}_{n\times n} . \tag{13}$$

where $a_{ij} = \alpha_i * \alpha_j$ for $1 \leq i, j \leq n$.

Let $\{\alpha_1, \cdots, \alpha_n\}$ be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. For each element $x \in \mathbb{F}_{2^n}$, its corresponding vector $\mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{F}_2^n$ can be uniquely represented as an integer $x_1 + 2x_2 + \cdots + 2^{n-1}x_n$. Conversely, each integer in the range $[0, 2^n - 1]$ corresponds to a vector in $\mathbb{F}_2^n$ by writing it as the 2-adic form. Clearly, the basis $\{\alpha_1, \cdots, \alpha_n\}$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ corresponds to the integers $1, 2, \cdots, 2^{n-1}$. To simplify the expression of APN functions, we use a sequence instead of a matrix to represent it. An example below is used to illustrate the expression.

Example 1. Let F be a quadratic APN function defined on $\mathbb{F}_{2^7}$ and $\mathfrak{A}$ be its corresponding APN algebra. Assume the matrix A of $\mathfrak{A}$ is

$$A = \begin{pmatrix} 0 & 2 & 4 & 8 & 16 & 32 & 64 \\ 2 & 0 & 48 & 35 & 76 & 51 & 69 \\ 4 & 48 & 0 & 1 & 2 & 15 & 104 \\ 8 & 35 & 1 & 0 & 71 & 126 & 13 \\ 16 & 76 & 2 & 71 & 0 & 62 & 28 \\ 32 & 51 & 15 & 126 & 62 & 0 & 70 \\ 64 & 69 & 104 & 13 & 28 & 70 & 0 \end{pmatrix} .$$

We represent A by the sequence of its nonzero elements of the upper-triangle matrix from left to right and top to bottom, i.e. [2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 15, 104, 71, 126, 13, 62, 28, 70].

4.1 By known APN functions

By Proposition 2, the nonzero elements of each row of A are linearly independent over $\mathbb{F}_2$. Therefore, we may fix the first row of A to be $a_{1i} = 2^{i-1}$ for $2 \leq i \leq n$. By choosing certain second row, and then let the computer do the search. This method is particularly efficient on the field $\mathbb{F}_{2^6}$. By a personal computer, it takes 3 hours to find all 13 quadratic APN functions in [10].

Except the above method, we find that new quadratic APN functions on $\mathbb{F}_{2^7}$ may be discovered using known APN functions. Indeed, on $\mathbb{F}_{2^7}$, we first represent the Gold APN function x^3 by its matrix form, and then fixing the first two rows and columns, and let the other entries run through $\mathbb{F}_{2^7}$ (note that all the diagonal elements are 0). Surprisingly, we find $30,000$ quadratic APN functions. After verifying the newness of $5,000$ of them, we obtain 285 new APN functions. It is entirely possible to get more new APN functions by verifying the remaining functions. In the following table, we list 10 of newly obtained functions. The complete computational results may be found in [19].

Table 4. New APN functions on $\mathbb{F}_{2^7}$

No.	APN Function
1	[2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 15, 104, 71, 126, 13, 62, 28, 70]
2	[2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 15, 42, 25, 70, 82, 4, 7, 53]
3	[2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 20, 65, 5, 115, 18, 113, 106, 62]
4	[2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 24, 15, 115, 84, 101, 41, 114, 4]
5	[2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 15, 124, 39, 71, 120, 22, 110, 12]
6	[2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 24, 126, 41, 106, 6, 111, 72, 40]
7	[2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 29, 60, 97, 82, 37, 100, 67, 66]
8	[2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 26, 88, 62, 106, 18, 122, 45, 8]
9	[2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 12, 71, 48, 86, 123, 46, 65, 37]
10	[2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 12, 78, 81, 121, 21, 23, 104, 76]

We need to mention that, the method to find new APN functions in this section is only useful for fields with small dimensions. For large fields, it is difficult to find APN functions either by exhaustive search or by fixing several rows and columns of some

known APN functions. Therefore, we need to find more properties of APN functions in order to get new examples, which is the topic of the following section.

4.2 By property of APN functions

Let u be a primitive element of $\mathbb{F}_{2^6}$. In [11], Dillon observed that, on the field $\mathbb{F}_{2^6}$, the switching neighbors of the APN function x^3 consists of two functions: x^3 and $x^3 + u^{11}x^6 + ux^9$. On the other hand, the switching neighbors of the Kim APN function $x^3 + x^{10} + ux^{24}$ consists of 11 functions, and we call them *Kim type* APN functions. It is pointed out in [11] that Kim type APN functions are related to partial spread differential sets $\mathcal{PS}^+$.

For the APN functions F in the switching neighbor of x^3, it is not difficult to see that $F(x) = F(wx) = F(w^2x)$ for all $x \in \mathbb{F}_{2^6}$, where $w = u^{(2^6-1)/3} \in \mathbb{F}_{2^6}$. We call an APN function which satisfies this property a *cube type* APN function. In the following, we show a method to discover cube type APN functions on the field $\mathbb{F}_{2^n}$ with n even, particularly, we find 10 new such functions on $\mathbb{F}_{2^8}$. We begin with the following property of cube type APN functions.

Proposition 3. *Let F be a quadratic cube type APN function on $\mathbb{F}_{2^n}$ with n is an even integer, and $\mathfrak{A} = (\mathbb{F}_{2^n}, +, *)$ be its APN algebra. Then we have*

$$x * wx = F(x),$$

$$wx * wy = x * y,$$

where $w = u^{\frac{2^n-1}{3}} \in \mathbb{F}_{2^n}$ and u is a primitive element of $\mathbb{F}_{2^n}$. Therefore, we have the following multiplication table. Note that $a + b = c$ below.

$*$	x	wx	w^2x
y	a	b	c
wy	c	a	b
w^2y	b	c	a

Proof. W.l.o.g. we may assume that $F(0) = 0$. For any $x \in \mathbb{F}_{2^n}$, we have $x * wx = F(x+wx)+F(x)+F(wx)+F(0) = F((1+w)x)+F(x)+F(x) = F(w^2x) = F(x)$. The second assertion follows similarly and we omit the proof. For the multiplication table, we only need to show that $a + b = c$, which is equivalent to $a + b + c = 0$. Actually, by $a = x * y, b = w * wy, c = x * w^y$, we have $a + b + c = x * (y + wy + w^y) = 0$ which completes the proof. □

Now, let F be a cube type function defined on $\mathbb{F}_{2^8}$. Choose a basis of $\mathbb{F}_{2^8}$ over $\mathbb{F}_2$ with the form $\{x_1, wx_1, \cdots, x_4, wx_4\}$, the matrix corresponding to F is then as follows. Note that, by the symmetry of the matrix, one may fill in the entries which do not list in the matrix.

Table 5. Cube type APN matrix in $\mathbb{F}_{2^8}$

$*$	x_1	wx_1	x_2	wx_2	x_3	wx_3	x_4	wx_4
x_1	0	t_1	a_1	b_1	a_2	b_2	a_3	b_3
wx_1	t_1	0	a_1+b_1	a_1	a_2+b_2	a_2	a_3+b_3	a_3
x_2			0	t_2	a_4	b_4	a_5	b_5
wx_2			t_2	0	a_4+b_4	a_4	a_5+b_5	a_5
x_3					0	t_3	a_6	b_6
wx_3					t_3	0	a_6+b_6	a_6
x_4							0	t_4
wx_4							t_4	0

By the above matrix representation of the cube type APN function on $\mathbb{F}_{2^8}$, we successfully discover 10 new such functions, which are listed below. The new 10 APN functions are presented in Table 4.2 below.

5 Properties of newly discovered APN functions

After obtaining many new quadratic APN functions, we need to study their properties. This section is devoted to discussing some interesting properties of these newly found functions.

Table 6. New APN functions on $\mathbb{F}_{2^8}$

No.	APN Function
1	[1, 6, 204, 20, 142, 72, 85, 204, 202, 154, 20, 85, 29, 8, 48, 30, 160, 61, 30, 46, 157, 160, 9, 123, 37, 37, 94, 203]
2	[1, 6, 204, 20, 142, 72, 85, 204, 202, 154, 20, 85, 29, 8, 48, 30, 160, 61, 30, 46, 157, 160, 34, 39, 209, 209, 246, 175]
3	[1, 6, 204, 20, 142, 72, 85, 204, 202, 154, 20, 85, 29, 8, 48, 30, 160, 61, 30, 46, 157, 160, 61, 140, 148, 148, 24, 198]
4	[1, 6, 204, 20, 142, 72, 85, 204, 202, 154, 20, 85, 29, 8, 48, 30, 160, 61, 30, 46, 157, 160, 69, 146, 3, 3, 145, 227]
5	[1, 6, 204, 20, 142, 72, 85, 204, 202, 154, 20, 85, 29, 8, 48, 30, 160, 61, 30, 46, 157, 160, 113, 168, 234, 234, 66, 177]
6	[1, 6, 204, 20, 142, 72, 85, 204, 202, 154, 20, 85, 29, 8, 48, 30, 160, 61, 30, 46, 157, 160, 115, 82, 127, 127, 45, 159]
7	[1, 6, 204, 20, 142, 72, 85, 204, 202, 154, 20, 85, 29, 8, 48, 30, 160, 61, 30, 46, 157, 160, 156, 115, 112, 112, 3, 193]
8	[1, 6, 204, 20, 142, 72, 85, 204, 202, 154, 20, 85, 29, 8, 48, 30, 160, 61, 30, 46, 157, 160, 252, 221, 182, 182, 107, 26]
9	[1, 6, 204, 20, 142, 72, 85, 204, 202, 154, 20, 85, 29, 8, 48, 30, 160, 73, 30, 46, 233, 160, 98, 33, 114, 114, 83, 4]
10	[1, 6, 204, 20, 142, 72, 85, 204, 202, 154, 20, 85, 29, 8, 48, 30, 160, 105, 30, 46, 201, 160, 188, 223, 242, 242, 45, 5]

5.1 Γ-, Δ-ranks and order of multiplier group

We first give the computational results of the Γ-, Δ-ranks and the order of the multiplier groups of the newly obtained quadratic APN functions in the following two tables.

Table 7. Invariant of New APN functions on $\mathbb{F}_{2^7}$

No.	Γ-rank	Δ-rank	$\sharp\mathcal{M}(G_F)$
1	4048	212	2^7
2	4048	212	2^7
3	4048	212	2^7
4	4046	212	2^7
5	4048	212	2^7
6	4048	212	2^7
7	4046	212	2^7
8	4046	212	2^7
9	4050	212	2^7
10	4048	212	2^7

One may see in Table 7 that the order of multiplier group of G_F are all 2^7. Actually this is true for all found $30,000$ APN functions on this field. By Result 2, if an APN

Table 8. Invariants of the New APN functions on $\mathbb{F}_{2^8}$

No.	Γ-rank	Δ-rank	$\sharp\mathcal{M}(G_F)$
1	14040	438	$2^8 \cdot 3$
2	14044	438	$2^8 \cdot 3$
3	14036	438	$2^8 \cdot 3$
4	14048	438	$2^8 \cdot 3$
5	14040	438	$2^8 \cdot 3$
6	14040	438	$2^8 \cdot 3$
7	14042	438	$2^8 \cdot 3$
8	14040	438	$2^8 \cdot 3$
9	14040	438	$2^{10} \cdot 3$
10	14040	438	$2^{10} \cdot 3^2 \cdot 5$

functions is CCZ-equivalent to a power function (resp. a polynomial in $\mathbb{F}_2[x]$), it should have $7 \cdot (2^7 - 1) \mid \sharp\mathcal{M}(G_F)$ (resp. $7 \mid \sharp\mathcal{M}(G_F)$). It is clear that these newly found APN functions are not CCZ equivalent to any power mappings and any APN polynomials in $\mathbb{F}_2[x]$. In some sense, this shows the limit of searching APN functions according to the number of terms of their polynomial form since from the computational results most APN functions have many terms. Similarly, from Table 8, the newly obtained APN functions on $\mathbb{F}_{2^8}$ are not CCZ-equivalent to power functions and APN polynomials on $\mathbb{F}_2[x]$.

5.2 Classes of switching neighbors

For an APN function F on $\mathbb{F}_{2^n}$, we call the APN functions of the form $F(x) + uf(x)$ the *switching neighbors of F in the narrow sense*, where $u \in \mathbb{F}_{2^n}$ and f is a Boolean function. The *class* of the switching neighbors of F refers to all CCZ-inequivalent APN functions amongst them. In [13], the authors observed that, on $\mathbb{F}_{2^7}$, every APN functions has small switching classes (with size $1, 2$ or 3).

For the 285 newly found APN functions on $\mathbb{F}_{2^7}$, we compute their switching neighbors to verify the observation in [13]. It is found that the largest switching class has 3

inequivalent APN functions, which further confirm the observation in [13]. It is natural to ask the following question.

Problem 3. For APN functions on $\mathbb{F}_{2^n}$ with n is an odd integer. Whether there exists an APN function such that its switching class has large size (at least great than 3)?

6 Concluding remarks

It is well known that, for functions defined on $\mathbb{F}_{p^n}$, where p is an odd prime, the lowest possible differential uniformity is 1 and the functions achieving this value are called *perfect nonlinear* (PN). The quadratic perfect nonlinear functions are proven conceptually equivalent to commutative semifields. The 3-tuple $\mathfrak{A} = (\mathbb{F}_{p^n}, +, *)$ *commutative semifield* if $*$ satisfies commutative and distributive law, and for $x, y \in \mathbb{F}_{p^n}$, $x * y = 0$ if and only if $x = 0$ or $y = 0$. Obviously, the difference between semifield and APN algebra defined in this paper is the condition of $x * y = 0$. The characterization of quadratic APN functions using APN algebra is similar to the treatment of quadratic PN functions.

In this paper, on small fields, we use the relationship between quadratic APN functions and APN algebras, and with the help of a computer, to find 285 new quadratic APN functions on $\mathbb{F}_{2^7}$ and 10 new ones on $\mathbb{F}_{2^8}$, which is a remarkable contrast to the number of currently known such functions. By the searching techniques developed in Section 4, it is very hopeful to discover much more APN functions on small fields.

References

1. E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, Journal of Cryptology, 4(1): 3–72, (1991).
2. L. Budaghyan, C. Carlet and A. Pott, New classes of almost bent and almost perfect nonlinear polynomials, IEEE Transactions on Information Theory 52(3), (2006).
3. L. Budaghyan and C. Carlet, Classes of quadratic APN trinomials and hexanomials and related structures, IEEE Transactions on Information Theory 54 (5), 2354–2357, (2008).
4. L. Budaghyan, C. Carlet, G. Leander, Two Classes of Quadratic APN Binomials Inequivalent to Power Functions, IEEE Transactions on Information Theory 54(9), 4218-4229, (2008).

5. L. Budaghyan and C. Carlet, Constructing new APN functions from known ones, Finite Fields and Their Applications 15(2), 150–159, (2009).
6. C. Bracken, E. Byrne, N. Markin, and G. McGuire, New families of quadratic almost perfect nonlinear trinomials and multinomials, Finite Fields Appl. 14, 703–714, 2008.
7. C. Bracken, E. Byrne, N. Markin and G. McGuire, A few more quadratic APN functions, Cryptography and Communications 3 (1), 43-53, 2011.
8. C. Carlet, P. Charpin and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, Designs, Codes and Cryptography, 15, 125–156, (1998).
9. F. Chabaud and S. Vaudenay, Links between differential and linear cryptanalysis, in Advances in Cryptology- EUROCRYPT 94, LNCS Vol. 94, 356–365, (1995).
10. J. F. Dillon, APN Polynomials and Related Codes, Polynomials over Finite Fields and Applications, Banff International Research Station, Nov. (2006).
11. J. F. Dillon, APN Polynomials: An Update, Fq9, International Conference on Finite Fields and their Applications, Jul. (2009).
12. Y. Edel, G. Kyureghyan, A. Pott, A new APN function which is not equivalent to a power mapping, IEEE Transaction on Information Theory 52(2), 744–747, (2006).
13. Y. Edel and A. Pott, A new almost perfect nonlinear function which is not quadratic, Advances in Mathematical Communications 3(1), 59–81, (2009).
14. Y. Edel, A. Pott, On Designs and Multiplier Groups Constructed from Almost Perfect Nonlinear Functions. IMA International Conference, 383–401, (2009).
15. Y. Edel, On quadratic APN functions and dimensional dual hyperovals, Design Codes and Cryptography 57(1), 35–44, (2010).
16. S. W. Golomb, G. Gong, Signal design for good correlation: For Wireless Communication, Cryptography, and Radar, Cambridge Press, (2005).
17. W. M. Kantor, Commutative semifields and symplectic spreads, Journal of Algebra 270(1), 96–114, (2003).
18. K. Nyberg, L. Knudsen: Provable Security Against Differential Cryptanalysis, CRYPTO 1992: 566-574,
19. Y. Tan, New quadratic APN functions on $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$, "https://ece.uwaterloo.ca/~y24tan/".
20. G. Weng, R. Feng, W. S. Qiu, On the ranks of bent functions, . Finite Fields and Their Applications 13 (4), 1096-1116, (2007).
21. S. Yoshiara, Equivalences of quadratic APN functions, Journal of Algebraic Combinatorics 35(3), 461-475, (2012).