On Quadratic Almost Perfect Nonlinear Functions and Their Related Algebraic Object

Guobiao Weng · Yin Tan · Guang Gong

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. They are also interesting as 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. By this characterization and with the help of a computer, we discovered 285 new (up to CCZ equivalence) quadratic APN functions on $\mathbb{F}_{2^7}$, which is a remarkable contrast to the currently known 17 such functions. Furthermore, 10 new quadratic APN functions on $\mathbb{F}_{2^8}$ are found. We propose some problems and conjectures based on the computational results.

Keywords Almost perfect nonlinear · 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 II) functions achieve the lowest possible differential uniformity for functions defined 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 all known families. It is conjectured that the list of power APN functions is complete (up to CCZ-equivalence, see the definition in Section II).

G. Weng
School of Mathematical Sciences, Dalian University of Technology, Liaoning 116024, China.
E-mail: gbweng@dlut.edu.cn

Y. Tan and G. Gong
Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada.
E-mail: {y24tan, ggong}@uwaterloo.ca
Table 1 Known power APN functions on \( \mathbb{F}_{2^n} \)

<table>
<thead>
<tr>
<th></th>
<th>Exponent ( d )</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gold</td>
<td>( 2^i + 1 )</td>
<td>( \gcd(i, n) = 1 )</td>
</tr>
<tr>
<td>Kasami</td>
<td>( 2^i - 2^i + 1 )</td>
<td>( \gcd(i, n) = 1 )</td>
</tr>
<tr>
<td>Welch</td>
<td>( 2^i + 3 )</td>
<td>( n = 2t + 1 )</td>
</tr>
<tr>
<td>Niho</td>
<td>( 2^t + 2^{(t/2) - 1} ), ( t ) even</td>
<td>( n = 2t + 1 )</td>
</tr>
<tr>
<td></td>
<td>( 2^t + 2^{(3t+1)/2} - 1 ), ( t ) odd</td>
<td>( n = 2t + 1 )</td>
</tr>
<tr>
<td>Inverse</td>
<td>( 2^i - 2 )</td>
<td>( n = 2t + 1 )</td>
</tr>
<tr>
<td>Dobbertin</td>
<td>( 2^i + 2^{i+2} + 2^i - 1 )</td>
<td>( n = 5t )</td>
</tr>
</tbody>
</table>

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 \( \omega \) has order 3 or 93; \( x^3 + \omega x^{36} \), where \( \omega \) 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 II).

Besides the method of generalizing sporadic APN functions into APN polynomials, in [5], the switching method is applied to construct new APN functions and the APN function \( x^3 + \text{Tr}(x^9) \) 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 \( \mathbb{F}_{2^5} \), one new on \( \mathbb{F}_{2^7} \) and eleven on \( \mathbb{F}_{2^9} \). 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 (a sporadic example on \( \mathbb{F}_{2^5} \) was found in [13]). Moreover, there is little knowledge about the existence of APN permutations on fields with even degrees, i.e. \( \mathbb{F}_{2^e} \). Until now, there is only one such function on \( \mathbb{F}_{2^e} \) was found by Dillon in [11]. This APN permutation is CCZ-equivalent to the quadratic APN function \( x^3 + u^{11} x^6 + ux^9 \) on \( \mathbb{F}_{2^e} \), where \( u \) is a primitive element of \( \mathbb{F}_{2^e} \). To discover more APN permutations on \( \mathbb{F}_{2^e} \) is called the *BIG APN Problem*. By Dillon’s method, finding more quadratic APN functions may give a hope to obtain APN permutations on \( \mathbb{F}_{2^e} \).

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 which will be introduced 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 \( F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n} \), in Theorem 1, we show that if \( F \) is a quadratic APN function, \( \mathfrak{A} = (\mathbb{F}_{2^n}^2, +, *) \) is an APN algebra, where \( x*y = F(x) + F(y) + F(x+y) + F(0) \).

Conversely, for any APN algebra \( \mathfrak{A} = (\mathbb{F}_{2^n}^2, +, *) \), a quadratic APN function can be defined through it (see (6)). This characterization enables us to give a unifying treatment of quadratic APN functions in terms of APN algebras.

Furthermore, in Section III, we present a matrix representation of the APN algebra, which can be applied to search for new (up to CCZ equivalence) 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 \( \mathbb{F}_8 \), \( \mathbb{F}_{27} \) and \( \mathbb{F}_{64} \).

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 \( \mathbb{F}_8 \). We should mention that this fact is also known by Yves Edel. Secondly, on \( \mathbb{F}_{27} \), we found 30,000 quadratic APN functions by a personal computer in two days. We randomly choose 5,000 of them to find new quadratic APN functions and test their newness, of which 285 new functions are found. We reasonably believe that more new ones may be found in the remaining 25,000 functions. Finally, on \( \mathbb{F}_{64} \), we test 500 quadratic APN functions, and 10 new ones are obtained. All these computations are done by a personal laptop, we expect that more APN functions may be quickly 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 the techniques how to search for new quadratic APN functions on small fields using the above characterization. The new quadratic APN functions on \( \mathbb{F}_{27}, \mathbb{F}_{64} \) and other computational results are presented in this Section as well. Based on the computational result, we also propose some open problems and conjectures. Finally, we give some concluding remarks in Section 5.

### 2 Preliminaries

In this Section, we give some 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

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

where \( |\cdot| \) denotes the cardinality for a set \( S \). We call

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

the differential uniformity of \( F \), or call \( F \) a differentially \( \Delta_F \)-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 \( F^W : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \rightarrow \mathbb{C} \) of \( F \) is defined by:

\[
F^W(a, b) := \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(aF(x)+bx)}
\]

where \( \text{Tr}(x) = \sum_{i=0}^{n-1} x^{2^i} \) denotes the absolute trace function. The multiset \( W_F := \{ F^W(a, b) : a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}\} \) 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 \( \max |W_F(a, b)| \geq 2^{(n+1)/2} \) when \( n \) is odd, and it is known \( \max |W_F(a, b)| \geq 2^{n/2+1} \) when \( n \) is even. We call \( F \) an almost bent (AB) function if

<table>
<thead>
<tr>
<th>( n )</th>
<th>( \sharp ) of APN in [13]</th>
<th>( \sharp ) of newly found APN in this paper</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>14</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>17</td>
<td>( \geq 285 )</td>
</tr>
<tr>
<td>8</td>
<td>23</td>
<td>10</td>
</tr>
</tbody>
</table>
Let $F^{W}(a,b) \in \{0, \pm 2^{(n+1)/2}\}$ 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 must be an AB function ([8]).

Finally, we call the function $F$ 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 $G_{F} = \{(x, F(x)) : x \in \mathbb{F}_{2^{n}}\}$ and $G_{G} = \{(x, G(x)) : x \in \mathbb{F}_{2^{n}}\}$ are affine equivalent, that is, there exists an affine isomorphism $L$ of $\mathbb{F}_{2^{n}} \times \mathbb{F}_{2^{n}}$ such that $L(G_{F}) = G_{G}$. It is well known that EA equivalence implies CCZ equivalence, but not vice 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 $x = (x_{1}, \cdots, x_{n}) \in \mathbb{F}_{2}^{n}$ such that $x = x_{1}\alpha_{1} + \cdots + x_{n}\alpha_{n}$. We use the notation $x$ 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 $C_{F} \in \mathbb{F}_{2}^{(2n+1) \times 2n}$ as follows:

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

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 $x, F(x)$ are regarded as elements in $\mathbb{F}_{2}^{n}$ as explained above). Let $C_{F}$ be the linear code generated by $C_{F}$. We have the following result.

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

There are some invariants of APN functions under CCZ-equivalence. For instance, the differential spectrum and extended Walsh spectrum of APN functions. The same 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 convenience, 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

$$G_{F} \cdot G_{F} = 2^{n} \cdot (0,0) + 2 \cdot D_{F} \quad (2)$$

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 $I'$- and $\Delta'$- 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 $\text{Aut}(\mathbb{F}_{2^{n}} \times \mathbb{F}_{2^{n}})$, 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.
Let $F$ be an APN function on $\mathbb{F}_{2^n}$ and $v = 2^k M(G_F)$. 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 parameters is that they are 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 will be discussed in Section IV. First, we give the definition of the APN algebra.

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

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

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

**Proposition 1** Let $\mathfrak{A} = (\mathbb{F}_{2^n}, +, \ast)$ 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 $x \ast y = xAy^T$, where $x, y$ are the corresponding vectors of $x, y$ in $\mathbb{F}_{2^n}$.

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

$$x \ast y = \left(\sum_{i=1}^{n} x_i \alpha_i\right) \ast \left(\sum_{i=1}^{n} y_i \alpha_i\right)$$

$$= \sum_{i,j=1}^{n} x_i y_j (\alpha_i \ast \alpha_j)$$

$$= xAy^T.$$

We finish the proof. $\square$

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 $\mathfrak{A} = (\mathbb{F}_{2^n}, +, \ast)$ 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 exist $(t_2, \cdots, t_n) \in \mathbb{F}_2^{n-1}$ such that $t_2 a_{12} + \cdots + t_n a_{1n} = 0$. Substituting $a_{ij} = \alpha_i \ast \alpha_j$ we have

$$0 = t_2 \alpha_1 \ast \alpha_2 + \cdots + t_n \alpha_1 \ast \alpha_n$$

$$= \alpha_1 \ast (t_2 \alpha_2 + \cdots + t_n \alpha_n).$$

Then, by the definition of APN algebra, we have $t_2 \alpha_2 + \cdots + t_n \alpha_n$ equals 0 or $\alpha_1$. 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. $\square$
Furthermore, for simplicity, we write the matrix $A$ as in the form $A = B + B^T$, where

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

### 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

$$F(x) = xBx^T \tag{6}$$

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

$$x *_{F} y = y *_{F} x \quad \text{(commutative law)},$$

$$x *_{F} (y + z) = x *_{F} y + x *_{F} z \quad \text{(distributive law)}.$$

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

$$0 = \Delta_a(x) = xBa^T + aBx^T = xBa^T + (aBx^T)^T = x(B + B^T)a^T = xAa^T = x * a.$$

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. \hfill $\square$

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

$$F(x) = \sum_{i,j=1}^{n} x_{i}x_{j} (\alpha_{i} * \alpha_{j}), \quad x = (x_1, \cdots, x_n).$$
Two APN algebras $\mathfrak{A}_1 = (F_{2^n}, +, *_1)$ and $\mathfrak{A}_2 = (F_{2^n}, +, *_2)$ 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 $x, y \in F_{2^n}$. 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 $F_{2^n}$. If $F_1$ and $F_2$ are EA equivalent, their corresponding APN algebras $\mathfrak{A}_1 = (F_{2^n}, +, *_{F_1})$ and $\mathfrak{A}_2 = (F_{2^n}, +, *_{F_2})$ are isomorphic. Conversely, if two APN algebras $\mathfrak{A}_1 = (F_{2^n}, +, *_1)$ and $\mathfrak{A}_2 = (F_{2^n}, +, *_2)$ 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

$$F_1 \circ A_1 + A_3 = A_2 \circ F_2$$  \hspace{1cm} (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

$$F_1(A_1(x)) + F_1(A_1(y)) = F_1(A_1(x + y)) + F_1(A_1(0))$$

$$L_2(F_2(x) + F_2(y) + F_2(x + y) + F_2(0)).$$

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

$$F_1(L_1(x)) + F_1(L_1(y)) = L_2(F_2(x) + F_2(y) + F_2(x + y) + F_2(0)),$$

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. \hfill $\Box$

### 3.3 A construction of APN algebra $(F_{2^n}, +, *)$

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

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

$$x * y = \left( 0d + bc, t_0(ac^2 + a^2 + b) + t_1(ad^2 + cd^2 + a^2 + a^2) + t_2(ba^2 + db^2 + a^2) \right),$$

where the polynomial

$$t_0a^{s+1}x + t_1x^2 + t_2x + t_3 \in F_{2^n}[x]$$

has no zeros over $F_{2^n}$. Then $\mathfrak{A} = (F_{2^n}, +, *)$ is an APN algebra.
The commutative and distributive law can be verified easily for $\mathfrak{l}$. It is also clear that $x \ast y = 0$ if $x = y$ or one of $x, y$ is zero. Now, assume that $x \ast y = 0$, we need to show that either $x = y$ or one of $x, y$ is 0. W.l.o.g. suppose $x \neq 0$, then

$$0 = ad + be,$$

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

By (11), the determinant

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

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

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

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

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

By the assumption that the polynomial $t_0a^{2^r+1} + t_1a^{2^r}b + t_2ab^{2^r} + t_3b^{2^r+1}$ has no zero over $\mathbb{F}_{2k}$, we can only have $t + t^2 = 0$, which follows that $t \in \mathbb{F}_{2 \text{gcd}(s, n)} = \mathbb{F}_2$. Now, from $c = ta, d = tb$, we have: $x = y$ when $t = 1$ and $y = 0$ when $t = 0$. We finish the proof. \hfill $\square$

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

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

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 monomial 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 $\Gamma$-rank, $\Delta$-rank, $\text{Dev}(G_F)$, $\text{Dev}(D_F)$ and $\mathcal{M}(G_F)$ are defined in Section 2.2. The symbol “-” means that our computer cannot calculate that parameter.

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].

<table>
<thead>
<tr>
<th>$n$</th>
<th>$\Gamma$-rank</th>
<th>$\Delta$-rank</th>
<th>$\text{Dev}(G_F)$</th>
<th>$\text{Dev}(D_F)$</th>
<th>$\mathcal{M}(G_F)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>1140</td>
<td>94</td>
<td>$2^{18} \cdot 3^4 \cdot 7$</td>
<td>$2^{18} \cdot 3^4 \cdot 7$</td>
<td>$2^{18} \cdot 3^4 \cdot 7$</td>
</tr>
<tr>
<td>8</td>
<td>13200</td>
<td>414</td>
<td>-</td>
<td>-</td>
<td>$2^{10} \cdot 3^2 \cdot 5$</td>
</tr>
<tr>
<td>10</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>$2^{10} \cdot 3^2 \cdot 5 \cdot 11$</td>
</tr>
</tbody>
</table>
4 New quadratic APN functions

In this Section, we will present the new quadratic APN functions discovered by a computer on $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$. Some interesting properties of these newly found functions are discussed as well. Firstly, we explain the techniques to discover these new 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

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

(13)

where $a_{ij} = \alpha_i \ast \alpha_j$ 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 $x = (x_1, \cdots, x_n) \in \mathbb{F}_{2^n}^n$ can be uniquely represented as an integer $x = 2x_1 + 2x_2 + \cdots + 2^{n-1}x_n$. Conversely, each integer in the range $[0, 2^n - 1]$ corresponds to a vector in $\mathbb{F}_{2^n}^n$ 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 $1, 2, \cdots, 2^{n-1}$. 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 $a_{11} = 2^{i-1}$ for $2 \leq i \leq n$. By choosing certain second row, and then let the computer do the search. As a result, many new quadratic APN functions on $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$ are found, which will be presented in Tables 4 and 5 below. 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 New quadratic APN functions on $\mathbb{F}_{2^7}$

Firstly, we give newly discovered quadratic APN functions on $\mathbb{F}_{2^7}$. By fixing the first row of the matrix $A$ in (13) to be $\{0, 2, 4, 8, 16, 32, 64\}$, and choosing the second row to be $\{2, 0, 48, 35, 76, 51, 69\}$, we found 30,000 quadratic APN functions in two days. After spending seven days on verifying their newness (up to CCZ equivalence) of 5,000 of them, we obtain 285 new ones, which is a remarkable contrast to the currently known 17 such functions! We believe that the remaining 25,000 functions may still yield more new ones.

Instead of listing all 285 new APN functions, we give 10 of them in Table 4 to illustrate their properties, please refer to [19] for a complete list of the computational results. The $I$-, $\Delta$-ranks, the order of the multiplier groups $\mathcal{M}(G_F)$ are computed as well.

Based on the computational results, we discuss some properties of newly obtained APN functions as follows.
Table 4 New APN functions on $\mathbb{F}_2^7$

<table>
<thead>
<tr>
<th>No.</th>
<th>APN Function</th>
<th>$\Gamma$-rank</th>
<th>$\Delta$-rank</th>
<th>$\mathcal{M}(G_F)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>${2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 15, 104, 71, 126, 13, 62, 28, 70}$</td>
<td>4048</td>
<td>212</td>
<td>2 $^\dagger$</td>
</tr>
<tr>
<td>2</td>
<td>${2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 15, 42, 25, 70, 82, 4, 7, 53}$</td>
<td>4048</td>
<td>212</td>
<td>2 $^\dagger$</td>
</tr>
<tr>
<td>3</td>
<td>${2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 24, 15, 124, 39, 71, 120, 22, 110, 12}$</td>
<td>4046</td>
<td>212</td>
<td>2 $^\dagger$</td>
</tr>
<tr>
<td>4</td>
<td>${2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 15, 124, 39, 71, 120, 22, 110, 12}$</td>
<td>4048</td>
<td>212</td>
<td>2 $^\dagger$</td>
</tr>
<tr>
<td>5</td>
<td>${2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 15, 124, 39, 71, 120, 22, 110, 12}$</td>
<td>4046</td>
<td>212</td>
<td>2 $^\dagger$</td>
</tr>
<tr>
<td>6</td>
<td>${2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 24, 126, 41, 106, 6, 111, 72, 40}$</td>
<td>4046</td>
<td>212</td>
<td>2 $^\dagger$</td>
</tr>
<tr>
<td>7</td>
<td>${2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 24, 126, 41, 106, 6, 111, 72, 40}$</td>
<td>4046</td>
<td>212</td>
<td>2 $^\dagger$</td>
</tr>
<tr>
<td>8</td>
<td>${2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 24, 126, 41, 106, 6, 111, 72, 40}$</td>
<td>4046</td>
<td>212</td>
<td>2 $^\dagger$</td>
</tr>
<tr>
<td>9</td>
<td>${2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 12, 11, 48, 86, 123, 46, 66, 37}$</td>
<td>4050</td>
<td>212</td>
<td>2 $^\dagger$</td>
</tr>
<tr>
<td>10</td>
<td>${2, 4, 8, 16, 32, 64, 48, 35, 76, 51, 69, 1, 2, 12, 11, 48, 86, 123, 46, 66, 37}$</td>
<td>4048</td>
<td>212</td>
<td>2 $^\dagger$</td>
</tr>
</tbody>
</table>

4.1.1 AB function are EA equivalent to a PP

It is conjectured in [8] that any AB function is EA equivalent to a permutation. A counter example (with algebraic degree 3) to this conjecture was given in [2, Theorem 1]. Since quadratic APN functions on fields with odd degrees are AB functions, for each 285 newly discovered APN function $F$ on $\mathbb{F}_2^7$, by a computer, we may find a linearized polynomial $L \in \mathbb{F}_2^7[x]$ such that $F + L$ is a permutation. Therefore, we revise the conjecture in [8] as follows.

Conjecture 1 Each quadratic AB function is EA-equivalent to a permutation.

4.1.2 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 $\mathbb{F}_2^7$, there only have small switching classes (with size 1, 2 or 3), while, on $\mathbb{F}_2^8$, there is one large switching class (with size 17).

For the 285 newly found APN functions on $\mathbb{F}_2^7$, we compute their switching neighbors and further confirm the aforementioned observation, i.e. there is no large switching classes (the largest class has 3 inequivalent APN functions).

4.1.3 Order of $\mathcal{M}(G_F)$

One may see in Table 4 that the order of multiplier group of $G_F$ are all $2^7$. Actually this is true for all found 30,000 APN functions. By Result 2, these newly found APN functions are not CCZ equivalent to any power mappings and they are not in $\mathbb{F}_2[x]$. This shows the limit of searching APN functions according to the number of terms of their polynomial form as from the computational results most APN functions have many terms.

4.2 New quadratic APN functions on $\mathbb{F}_2^8$

The new 10 APN functions are presented in Table 5 below. These functions are obtained by choosing the first row of $A$ in (13) to be $\{0, 1, 6, 204, 20, 142, 75, 85\}$ and the second row to be $\{1, 0, 204, 202, 154, 20, 85, 29\}$. We should mention that, on $\mathbb{F}_2^8$, a computer takes much more time to search for new APN functions. However, by choosing the second row more carefully, it is possible to find more quadratic APN functions. Comparing to number of APN functions found in $\mathbb{F}_2^7$, we conjecture there exist thousands of APN functions on $\mathbb{F}_2^8$. Finally, the 10 newly found APN functions on $\mathbb{F}_2^8$ cannot yield APN permutation using Dillon’s method described in [11].
Table 5 New APN functions on $\mathbb{F}_2^8$

<table>
<thead>
<tr>
<th>No.</th>
<th>APN Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1, 6, 204, 20, 142, 72, 85, 204, 202, 154, 20, 85, 29, 48, 30, 160, 61, 30, 46, 157, 160, 9, 123, 37, 37, 94, 203</td>
</tr>
<tr>
<td>2</td>
<td>1, 6, 204, 20, 142, 72, 85, 204, 202, 154, 20, 85, 29, 8, 48, 30, 160, 61, 30, 46, 157, 160, 14, 39, 209, 209, 246, 175</td>
</tr>
<tr>
<td>3</td>
<td>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, 24, 198</td>
</tr>
<tr>
<td>4</td>
<td>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, 24, 198</td>
</tr>
<tr>
<td>5</td>
<td>1, 6, 204, 20, 142, 72, 85, 204, 202, 154, 20, 85, 29, 8, 48, 30, 160, 61, 30, 46, 157, 160, 14, 39, 209, 209, 246, 175</td>
</tr>
<tr>
<td>6</td>
<td>1, 6, 204, 20, 142, 72, 85, 204, 202, 154, 20, 85, 29, 8, 48, 30, 160, 61, 30, 46, 157, 160, 14, 39, 209, 209, 246, 175</td>
</tr>
<tr>
<td>7</td>
<td>1, 6, 204, 20, 142, 72, 85, 204, 202, 154, 20, 85, 29, 8, 48, 30, 160, 61, 30, 46, 157, 160, 14, 39, 209, 209, 246, 175</td>
</tr>
<tr>
<td>8</td>
<td>1, 6, 204, 20, 142, 72, 85, 204, 202, 154, 20, 85, 29, 8, 48, 30, 160, 61, 30, 46, 157, 160, 14, 39, 209, 209, 246, 175</td>
</tr>
<tr>
<td>9</td>
<td>1, 6, 204, 20, 142, 72, 85, 204, 202, 154, 20, 85, 29, 8, 48, 30, 160, 61, 30, 46, 157, 160, 14, 39, 209, 209, 246, 175</td>
</tr>
<tr>
<td>10</td>
<td>1, 6, 204, 20, 142, 72, 85, 204, 202, 154, 20, 85, 29, 8, 48, 30, 160, 61, 30, 46, 157, 160, 14, 39, 209, 209, 246, 175</td>
</tr>
</tbody>
</table>

Table 6 Invariants of the New APN functions on $\mathbb{F}_2^8$

<table>
<thead>
<tr>
<th>No.</th>
<th>$\Gamma$-rank</th>
<th>$\Delta$-rank</th>
<th>$\sharp M(\mathbb{F}_p)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>14040</td>
<td>438</td>
<td>$2^6$ - 3</td>
</tr>
<tr>
<td>2</td>
<td>14044</td>
<td>438</td>
<td>$2^6$ - 3</td>
</tr>
<tr>
<td>3</td>
<td>14036</td>
<td>438</td>
<td>$2^6$ - 3</td>
</tr>
<tr>
<td>4</td>
<td>14048</td>
<td>438</td>
<td>$2^6$ - 3</td>
</tr>
<tr>
<td>5</td>
<td>14040</td>
<td>438</td>
<td>$2^6$ - 3</td>
</tr>
<tr>
<td>6</td>
<td>14040</td>
<td>438</td>
<td>$2^6$ - 3</td>
</tr>
<tr>
<td>7</td>
<td>14032</td>
<td>438</td>
<td>$2^6$ - 3</td>
</tr>
<tr>
<td>8</td>
<td>14040</td>
<td>438</td>
<td>$2^6$ - 3</td>
</tr>
<tr>
<td>9</td>
<td>14040</td>
<td>438</td>
<td>$2^6$ - 3</td>
</tr>
<tr>
<td>10</td>
<td>14040</td>
<td>438</td>
<td>$2^6$ - 3</td>
</tr>
</tbody>
</table>

5 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 $\mathfrak{A} = (\mathbb{F}_{p^n}, +, \cdot)$ commutative semifield if $\cdot$ satisfies commutative and distributive law, and for $x, y \in \mathbb{F}_{p^n}$, $x \cdot y = 0$ 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 $x \cdot y = 0$. 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.

After finishing this work, we were informed by a reviewer that a similar work has been done by Y. Yu, M. Wang and Y. Li. We verified the CCZ equivalence of our APN functions on $\mathbb{F}_2^7$ with theirs, and find that 99 ones are equivalent to theirs. The complete test of our 285 functions on $\mathbb{F}_2^7$ will take much more time.

References

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).
19. Y. Tan, New quadratic APN functions on $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$, “https://ece.uwaterloo.ca/~y24tan/”.