Des. Codes Cryptogr. (2014) 73:587–600
DOI 10.1007/s10623-014-9955-3

A matrix approach for constructing quadratic APN functions

Yuyin Yu · Mingsheng Wang · Yongqiang Li

Received: 30 August 2013 / Revised: 12 February 2014 / Accepted: 3 March 2014 /
Published online: 28 March 2014

Abstract A one to one correspondence is given between quadratic homogeneous APN functions and a special kind of matrices which we call as QAM's. By modifying the elements of a known QAM, new quadratic APN functions can be constructed. Based on the nice mathematical structures of the QAM's, an efficient algorithm for constructing quadratic APN functions is proposed. On $\mathbb{F}_{2^7}$, we have found 471 new CCZ-inequivalent quadratic APN functions, which is 20 times more than the number of the previously known ones. Before this paper, It is only found 23 classes of CCZ-inequivalent APN functions on $\mathbb{F}_{2^8}$. With the method of this paper, we have found 2,252 new CCZ-inequivalent quadratic APN functions, and this number is still increasing.

Keywords Quadratic functions · APN, EA-equivalence · CCZ-equivalence

Mathematics Subject Classification 06E30 · 11T06 · 94A60

1 Introduction

Low differentially uniform permutations are very useful in cryptography, they can provide good resistance against differential attack. For example, the advanced encryption standard (AES) [12] uses a differentially 4-uniform permutation as its substitution box (S-box). The differentially 4-uniform permutation is the best choice for now due to the lack of differentially 2-uniform permutations on $\mathbb{F}_{2^8}$. For clarity, we first introduce the following definitions.

This is one of several papers published in *Designs, Codes and Cryptography* comprising the "Special Issue on Coding and Cryptography".

Y. Yu · M. Wang (✉) · Y. Li
The State Key Laboratory of Information Security, Institute of Information Engineering,
Chinese Academy of Sciences, Beijing 100093, China
e-mail: mingsheng_wang@aliyun.com

Definition 1 A mapping $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ is called differentially $\delta(F)$- uniform if

$$\delta(F) = \max_{a \in \mathbb{F}_{2^n}^{\star}, b \in \mathbb{F}_{2^n}} \# \Delta_F(a, b),$$

where $\Delta_F(a, b) = \{x \in \mathbb{F}_{2^n} : F(x + a) + F(x) = b\}$, and $\#\Delta_F(a, b)$ is the cardinality of $\Delta_F(a, b)$. If $\delta(F) = 2$, F is called almost perfect nonlinear (APN) [1].

Definition 2 [11] Let F and F' be two functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$.

(i) F and F' are Extended affine equivalent (EA-equivalent) if

$$F'(x) = A_1(F(A_2(x))) + A_3(x),$$

where A_1 and A_2 are affine permutations on $\mathbb{F}_{2^n}$, and A_3 is an affine function on $\mathbb{F}_{2^n}$.

(ii) F and F' are Carlet–Charpin–Zinoviev equivalent (CCZ-equivalent) if there exists an affine permutation which maps G_F onto $G_{F'}$, where $G_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ is the graph of F, and $G_{F'}$ is the graph of F'.

Note that $\delta(F)$ is always even, and APN functions provide optimal resistance against differential attack. The terminology APN was introduced by Nyberg and Knudsen [23] in 1992. Carlet, Charpin and Zinoviev proved that if a function is APN, then its CCZ-equivalent functions are all APN. CCZ-equivalence is a generalization of EA-equivalence. A function $F(x) = \sum_{j=0}^{2^n-1} c_j x^j \in \mathbb{F}_{2^n}[x]$ is called quadratic if the maximum Hamming weight of the binary expansion of j with $c_j \neq 0$ equals 2. According to Yoshiara's results [24], two quadratic APN functions are CCZ-equivalent if and only if they are EA-equivalent.

An APN function is new if it is not CCZ equivalent to any known ones. For a long time, finding new APN functions is an important research topic in cryptography. In recent years, most of the new APN functions found are quadratic [2–9,13–20]. For a systematic knowledge of APN functions, the readers can turn to [10].

Our work was motivated by a recent breakthrough on APN functions. In 2009, Dillon et al. [4,5,13] found an APN permutation in dimension six, which is the first APN permutation in even dimension. Their idea can be summarized as follows: firstly, finding an APN function, and then checking whether this APN function is CCZ-equivalent to a permutation or not. Thus, if we want to find new APN permutations in even dimensions, we must find new APN functions first.

Our aim is to find as many new APN functions as possible, especially on $\mathbb{F}_{2^8}$. Then we will check wether these new APN functions are CCZ-equivalent to some permutations. If some of these functions are CCZ-equivalent to permutations, then this will prove the existence of APN permutations on $\mathbb{F}_{2^8}$.

The contributions of this paper are as follows. In Sect. 2, a one to one correspondence is given between quadratic homogeneous APN functions and QAMs (see definition 5 in Sect. 2). In Sect. 3, some relations are proposed between quadratic homogeneous functions and their corresponding matrices, in particular, some properties of QAMs are given. These QAMs have nice mathematical structures and constructing QAMs is easier than constructing quadratic APN functions directly. In Sect. 4, based on some properties of the QAMs, we have designed an efficient algorithm to search for the new APN functions. Before this paper, the scholars [13,16] have found 19 and 23 classes of CCZ-inequivalent APN functions on $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$ respectively. With the algorithm of this paper, we have found more than 471 new CCZ-inequivalent APN functions on $\mathbb{F}_{2^7}$, and more than 2252 new CCZ-inequivalent quadratic APN functions on $\mathbb{F}_{2^8}$. The number of CCZ-inequivalent quadratic APN functions on $\mathbb{F}_{2^8}$ is still arising. We have checked all these new APN functions on $\mathbb{F}_{2^8}$, none of them is CCZ-equivalent to a permutation.

2 Notation and basic ideas

2.1 Notation

Let n be a positive integer, $\mathbb{F}_{2^n}$ be a finite field with 2^n elements, and $\mathbb{F}_{2^n}[x]$ be the polynomial ring in variable x over $\mathbb{F}_{2^n}$.

Definition 3 Quadratic functions on $\mathbb{F}_{2^n}$ without linear and constant terms are called quadratic homogeneous functions.

Definition 4 [21] Two bases $\{\alpha_1, \dots, \alpha_n\}$ and $\{\theta_1, \theta_2, \dots, \theta_n\}$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ are said to be dual if for $1 \le u, j \le n$ we have

$$\mathrm{Tr}(\alpha_u \theta_j) = \begin{cases} 0 \text{ for } & u \ne j; \\ 1 \text{ for } & u = j. \end{cases}$$

We will use the following convention and notation throughout the paper.

(i) For positive integers r, s, $\mathbb{F}_{2^n}^{r\times s}$ denotes the space of $r \times s$ matrices over $\mathbb{F}_{2^n}$. For a matrix A, let $A[i]$ be the ith row of A, $A[i, j]$ be the (i, j) entry of A, and $B =$ Submatrix$(A, 1, 1, r, c)$ the $r \times c$ submatrix of A consisting of the first r rows and the first c columns.

(ii) Suppose $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ is a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, and $\{\theta_1, \theta_2, \dots, \theta_n\}$ is its dual basis. Let $M_\alpha \in \mathbb{F}_{2^n}^{n\times n}$ and $M_\theta \in \mathbb{F}_{2^n}^{n\times n}$ with $M_\alpha[i, u] = \alpha_u^{2^{i-1}}$ and $M_\theta[i, u] = \theta_u^{2^{i-1}}$ for $1 \le u, i \le n$. Then $M_\alpha^T M_\theta = (\mathrm{Tr}(\alpha_u \theta_j))_{n\times n}$ for $1 \le u, j \le n$, so $M_\alpha^T M_\theta = I_n$, where I_n is the $n \times n$ identity matrix. Thus $M_\theta^{-1} = M_\alpha^T$, where M_α^T is the transpose of M_α.

(iii) Suppose $\eta_1, \eta_2, \dots, \eta_m \in \mathbb{F}_{2^n}$ $(m, n \ge 1)$, and $B = (\eta_1, \eta_2, \dots, \eta_m) \in \mathbb{F}_{2^n}^m$. Let Span$(B)$=Span$(\eta_1, \eta_2, \dots, \eta_m)$ be the subspace spanned by $\{\eta_1, \eta_2, \dots, \eta_m\}$ over $\mathbb{F}_2$. The rank of B over $\mathbb{F}_2$, denoted as $\mathrm{Rank}_{\mathbb{F}_2}(B)$, is defined as the dimension of Span(B) over $\mathbb{F}_2$. Suppose $\eta_i = \sum_{j=1}^n \lambda_{i,j}\alpha_j$ for $1 \le i \le m$, where $\lambda_{i,j} \in \mathbb{F}_2$ for all i, j. Define an $m \times n$ matrix $\Lambda = (\lambda_{i,j})_{m\times n}$. Then $\mathrm{Rank}_{\mathbb{F}_2}(B)$ equals to the rank of Λ.

Now we introduce a class of matrices which will play an important role in the present paper.

Definition 5 Let $H = (h_{u,v})_{n\times n}$ be an $n \times n$ matrix over $\mathbb{F}_{2^n}$. H is called a quadratic APN matrix (**QAM**) if

(i) H is symmetric and the elements in its main diagonal are zero;

(ii) Every nonzero linear combination of the n rows (or "columns" because of H being symmetric) of H has rank $n - 1$.

2.2 One to one correspondence between quadratic homogeneous APN functions and QAMs

In order to prove Theorem 1 below, we need to give a matrix representation of quadratic homogeneous functions.

Let $F(x) = \sum_{1\le t<i\le n} c_{i,t}x^{2^{i-1}+2^{t-1}} \in \mathbb{F}_{2^n}[x]$ be a quadratic homogeneous function. We define an $n \times n$ matrix $E = (e_{i,t})_{n\times n}$ by setting

$$e_{i,t} = \begin{cases} c_{i,t} \text{ if } & i > t; \\ 0 \quad \text{if } & i \le t. \end{cases} \tag{1}$$

Let $X = (x^{2^0}, x^{2^1}, \dots, x^{2^{n-1}})^T$. Then we have

$$F(x) = X^T E X. \tag{2}$$

Let $x = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$, where $x_i \in \mathbb{F}_2$, $1 \le i \le n$. Then (2) can be written as

$$F(x) = \overline{x}^T M^T E M \overline{x}, \tag{3}$$

where $\overline{x} = (x_1, x_2, \dots, x_n)^T$, and $M = M_\alpha$.

Now for $F(x) = \sum_{1 \le t < i \le n} c_{i,t} x^{2^{i-1}+2^{t-1}} \in \mathbb{F}_{2^n}[x]$, let C_F be an $n \times n$ matrix with $C_F[t, i] = C_F[i, t] = c_{i,t}$ for $1 \le t < i \le n$, and $C_F[i, i] = 0$ for $1 \le i \le n$. Thus by definition of E, we have $C_F = E + E^T$.

Given a basis $\alpha = \{\alpha_1, \dots, \alpha_n\}$ for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, and let $M = M_\alpha$. For any quadratic homogeneous function $F(x)$, let $H = M^T C_F M$. Then H is a symmetric matrix over $\mathbb{F}_{2^n}$ with main diagonal elements zero.

Conversely, for a symmetric matrix H over $\mathbb{F}_{2^n}$ with main diagonal elements all zero, we can define a unique quadratic homogeneous function $F(x)$ such that $H = M^T C_F M$. $F(x)$ is called the quadratic function defined by H relative to the ordered basis α.

Based on (3), we can build a one to one correspondence between quadratic homogeneous APN functions and QAMs.

Theorem 1 *Let $F(x) = \sum_{1 \le t < i \le n} c_{i,t} x^{2^{i-1}+2^{t-1}} \in \mathbb{F}_{2^n}[x]$, C_F and M be defined as above, and $H = M^T C_F M$. Then, $\delta(F) = 2^k$ if and only if the smallest rank of any nonzero linear combination of the n rows of H is $n - k$. In particular, F is APN on $\mathbb{F}_{2^n}$ if and only if H is a QAM.*

Proof Let E and $\overline{x}$ be the same as in (1) and (3), and $a = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$, where $\overline{a} = (a_1, \cdots, a_n)^T \in \mathbb{F}_2^n \backslash \{0\}$. Let

$$D_a(x) = F(x + a) + F(x) + F(a).$$

Then $D_a(x)$ is a linear function. So $\delta(F) = 2^k$ if and only if

$$\max\{\dim_{\mathbb{F}_2}(\mathrm{Ker}(D_a)) \mid a \in \mathbb{F}_{2^n}^\star\} = k.$$

Based on (3), we have

$$\begin{aligned}
D_a(x) &= (\overline{x} + \overline{a})^T M^T E M (\overline{x} + \overline{a}) + \overline{x}^T M^T E M \overline{x} + \overline{a}^T M^T E M \overline{a} \\
&= \overline{x}^T M^T E M (\overline{x} + \overline{a} + \overline{x}) + \overline{a}^T M^T E M (\overline{x} + \overline{a} + \overline{a}) \\
&= \overline{x}^T M^T E M \overline{a} + \overline{a}^T M^T E M \overline{x} \\
&= \overline{x}^T M^T E M \overline{a} + (\overline{a}^T M^T E M \overline{x})^T \\
&= \overline{x}^T M^T (E + E^T) M \overline{a} \\
&= \overline{x}^T M^T C_F M \overline{a} \\
&= \overline{x}^T H \overline{a}.
\end{aligned}$$

By linear algebra, $D_a(x) = 0$ has 2^k solutions if and only if $\mathrm{Rank}_{\mathbb{F}_2}((H\overline{a})^T) = n - k$. $H\overline{a}$ is a nonzero linear combination of the n columns of H since $\overline{a} \in \mathbb{F}_2^n \backslash \{0\}$. Thus $\delta(F) = 2^k$ if and only if

$$D_a(x) = \overline{x}^T H \overline{a} = 0$$

has 2^k solutions for any $\overline{a} \in \mathbb{F}_2^n \backslash \{0\}$.

Note that H is symmetric, thus the above results implies the conclusion. □

The matrix H associated with $F(x)$ in Theorem 1 is called the matrix of $F(x)$ relative to the ordered basis $\{\alpha_1, \ldots, \alpha_n\}$.

Note that M is an invertible matrix over $\mathbb{F}_{2^n}$, so the correspondence between quadratic homogeneous APN functions and QAMs is one to one. It seems that another similar approach have been considered by Knuth and Edel, the readers can turn to Slides from the talk [14] for details.

Theorem 1 is very useful when we want to study the differential properties of the quadratic functions, and it can be generalized to $\mathbb{F}_{p^n}$, where p is any prime and n is a positive integer. In this paper, we use only this theorem to study the quadratic APN functions on $\mathbb{F}_{2^n}$.

3 Theoretical results

In this section, we give some theoretical results concerning relationship between quadratic homogeneous functions and their corresponding matrices. Since our aim is to construct new APN functions up to EA-equivalence, thus we need to understand EA-equivalence of two functions in terms of their corresponding matrices.

Let $F(x)$ be a given quadratic homogeneous function. First we study what happens to corresponding matrices when the ordered basis is changed. Let $\alpha = \{\alpha_1, \ldots, \alpha_n\}$ and $\beta = \{\beta_1, \ldots, \beta_n\}$ be two ordered bases for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Assume H_α and H_β are corresponding matrices for $F(x)$ relative to the α, β respectively. How are the matrices H_α and H_β related?

As we know, there is a unique invertible $n \times n$ matrix P such that

$$(\beta_1, \ldots, \beta_n) = (\alpha_1, \ldots, \alpha_n)P.$$

Hence we have $M_\beta = M_\alpha P$. So we have $H_\beta = M_\beta^T C_F M_\beta = P^T H_\alpha P$.

Conversely, assume that H', H are two $n \times n$ symmetric matrices with main diagonal elements all zeros such that $H' = P^T H P$ for an invertible matrix P over $\mathbb{F}_2$.

Let $F(x)$ be the quadratic function defined by H relative to the ordered basis α. Let $\gamma = \{\gamma_1, \ldots, \gamma_n\}$ be defined by $(\gamma_1, \ldots, \gamma_n) = (\alpha_1, \ldots, \alpha_n)P$. Then γ is a basis for $\mathbb{F}_{2^n}$, and $F(x)$ is also the quadratic function defined by H' relative to ordered basis γ.

Now let $F'(x)$ be the quadratic function defined by H' relative to α, then how are the functions $F(x)$ and $F'(x)$ related ? In order to answer this problem, we first note the following lemma.

Lemma 1 *Suppose $H = (h_{u,v})_{n\times n}$ is a symmetric matrix over $\mathbb{F}_{2^n}$ with $h_{u,u} = 0$ for all $1 \le u \le n$. Define a set $S = \{K = (k_{u,v})_{n\times n} \mid k_{u,v} + k_{v,u} = h_{u,v}$ for all $1 \le v \le u \le n\}$. Then*

(1) $W \in S$ if and only if $W + W^T = H$.

(2) If $W_1 + W_1^T = H$ and $W_2 + W_2^T = H$, then there exists a symmetric matrix A such that $W_2 = W_1 + A$.

Proof (1) is obvious, omitting it, we prove only (2) in the following. Let $W_1 + W_1^T = H$ and $W_2 + W_2^T = H$, then for any symmetric matrix A, we have

$$(W_1 + A) + (W_1 + A)^T = W_1 + W_1^T + A + A^T = W_1 + W_1^T = H,$$

which implies that $W_1 + A \in S$ for any symmetric matrix A.

Define a set $S' = \{W_1 + A \mid A \text{ is symmetric}\}$. Easy to see that $\#S' = 2^{n^2(n+1)/2} = \#S$, and for any $W \in S'$, we have $W + W^T = H$. Thus we have $S = S'$. So $W_2 \in S'$, Hence there exists a symmetric matrix A with $W_2 = W_1 + A$. □

Theorem 2 *Let $H \in \mathbb{F}_{2^n}^{n\times n}$ be a symmetric matrix with main diagonal elements all zero, and $P \in \mathbb{F}_2^{n\times n}$ be an invertible matrix. Suppose $H' = P^T HP$, then the quadratic functions defined by H and H' relative to an ordered basis α are EA-equivalent. In particular, H is a QAM if and only if H' is a QAM.*

Proof Let the functions defined by H and H' relative to α be $F(x) = \sum_{1\le t<i\le n} c_{i,t}x^{2^{i-1}+2^{t-1}}$, and $F'(x) = \sum_{1\le t<i\le n} c'_{i,t}x^{2^{i-1}+2^{t-1}}$ respectively.

Let $E = (e_{i,t})$, and $E' = (e'_{i,t})$ be two $n \times n$ matrices such that

$$e_{i,t} = \begin{cases} c_{i,t} & \text{if} \quad i > t; \\ 0 & \text{if} \quad i \le t, \end{cases} \text{ and } e'_{i,t} = \begin{cases} c'_{i,t} & \text{if} \quad i > t; \\ 0 & \text{if} \quad i \le t. \end{cases}$$

By (3), we have

$$F(x) = \overline{x}^T M^T EM\overline{x}, \text{ and } F'(x) = \overline{x}^T M^T E'M\overline{x},$$

where $\overline{x} = (x_1, x_2, \ldots, x_n)^T \in \mathbb{F}_2^n$.

Let $W = M^T EM$, and $W' = M^T E'M$. Then $W + W^T = H$, and $W' + W'^T = H'$, which implies that $P^T WP + P^T W^T P = P^T HP = H' = W' + W'^T$. According to Lemma 1, there exists a symmetric matrix $A = (a_{u,v})_{n\times n}$ such that $W' = P^T WP + A$. Thus we have $\overline{x}^T W'\overline{x} = \overline{x}^T(P^T WP + A)\overline{x}$. Hence

$$\begin{aligned} F'(x) &= \overline{x}^T M^T E'M\overline{x} = \overline{x}^T P^T M^T EMP\overline{x} + \overline{x}^T A\overline{x} \\ &= G(x) + \overline{x}^T A\overline{x}, \end{aligned} \tag{4}$$

where $G(x) = \overline{x}^T P^T M^T EMP\overline{x}$.

Since A is symmetric, we have

$$\overline{x}^T A\overline{x} = \sum_{u=1}^{n}\sum_{v=1}^{n} a_{u,v}x_u x_v = \sum_{u=1}^{n} a_{u,u}x_u^2 = \sum_{u=1}^{n} a_{u,u}x_u. \tag{5}$$

By (4) and (5), $F'(x)$ is EA-equivalent to $G(x)$. As for $G(x)$, we have

$$G(x) = \overline{x}^T P^T M^T EMP\overline{x} = \overline{y}^T M^T EM\overline{y} = F(y),$$

where $\overline{y} = (y_1, y_2, \ldots, y_n)^T = P\overline{x}$. So $G(x)$ is affine equivalent to $F(x)$. Thus $F'(x)$ is EA-equivalent to $F(x)$. □

We need the following result (Theorem 2.3 in [22]) when proving Lemma 3.

Lemma 2 [22] *Let $\{\theta_1, \theta_2, \ldots, \theta_n\}$ be any given basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, and let $L(x)$ be a linearized polynomial over $\mathbb{F}_{2^n}$. Then there exists a unique vector $(\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{F}_{2^n}^n$ such that*

$$L(x) = \sum_{j=1}^{n} \mathrm{Tr}(\theta_j x)\beta_j = \sum_{i=1}^{n}\left(\sum_{j=1}^{n} \beta_j\theta_j^{2^{i-1}}\right)x^{2^{i-1}}.$$

Moreover, let k be an integer such that $0 \le k \le n$, then $\dim_{\mathbb{F}_2}(\mathrm{Ker}(L)) = k$ if and only if $\mathrm{Rank}_{\mathbb{F}_2}\{\beta_1, \beta_2, \ldots, \beta_n\} = n - k$.

Lemma 3 *With notation as in Lemma 2. Every quadratic function $Q(x) \in \mathbb{F}_{2^n}[x]$ with $Q(0) = 0$ can be denoted as*

$$Q(x) = \sum_{1 \le v < u \le n} \mathrm{Tr}(\theta_u x)\mathrm{Tr}(\theta_v x)(\eta_{u,v} + \eta_{v,u}) + \sum_{u=1}^{n} \mathrm{Tr}(\theta_u x)\eta_{u,u} \tag{6}$$

$$= \sum_{1 \le t < i \le n} c_{i,t} x^{2^{i-1}+2^{t-1}} + \mathrm{Lin}(x), \tag{7}$$

where

$$c_{i,t} = \sum_{1 \le u,v \le n} \theta_u^{2^{i-1}} \theta_v^{2^{t-1}} (\eta_{v,u} + \eta_{u,v}),$$

$$\mathrm{Lin}(x) = \sum_{1 \le v < u \le n} (\eta_{u,v} + \eta_{v,u})\mathrm{Tr}(\theta_u \theta_v x^2) + \sum_{u=1}^{n} \mathrm{Tr}(\theta_u x)\eta_{u,u},$$

and

$$\eta_{u,v}\ (1 \le u, v \le n) \textit{ are some elements in } \mathbb{F}_{2^n}.$$

Proof According to Lemma 2, every quadratic function without constant term can be denoted as $Q(x) = \sum_{t=1}^{n} L'_t(x) x^{2^{t-1}}$, where $L'_t(x) = \sum_{u=1}^{n} \mathrm{Tr}(\theta_u x)\omega_{u,t}$ and $\omega_{u,t} \in \mathbb{F}_{2^n}$ for all $1 \le u, t \le n$. Then we have $Q(x) = \sum_{u=1}^{n} L_u(x)\mathrm{Tr}(\theta_u x)$, where $L_u(x) = \sum_{t=1}^{n} \omega_{u,t} x^{2^{t-1}}$. Again, according to Lemma 2, we have $L_u(x) = \sum_{v=1}^{n} \mathrm{Tr}(\theta_v x)\eta_{v,u}$, where $\eta_{v,u} \in \mathbb{F}_{2^n}$ such that $\omega_{u,t} = \sum_{v=1}^{n} \theta_v^{2^{t-1}} \eta_{v,u}$. Hence we have

$$\begin{aligned} Q(x) &= \sum_{u=1}^{n} L_u(x)\mathrm{Tr}(\theta_u x) \\ &= \sum_{u=1}^{n} \left(\sum_{v=1}^{n} \mathrm{Tr}(\theta_v x)\eta_{v,u})\mathrm{Tr}(\theta_u x \right) \\ &= \sum_{1 \le u,v \le n} \mathrm{Tr}(\theta_u x)\eta_{u,v}\mathrm{Tr}(\theta_v x) \\ &= \sum_{1 \le v < u \le n} \mathrm{Tr}(\theta_u x)\mathrm{Tr}(\theta_v x)(\eta_{u,v} + \eta_{v,u}) \\ &\quad + \sum_{u=1}^{n} \mathrm{Tr}(\theta_u x)\eta_{u,u} \\ &= \sum_{1 \le v < u \le n} \sum_{i=1}^{n} (\theta_u x)^{2^{i-1}} \sum_{t=1}^{n} (\theta_u x)^{2^{t-1}} (\eta_{u,v} + \eta_{v,u}) \\ &\quad + \sum_{u=1}^{n} \mathrm{Tr}(\theta_u x)\eta_{u,u} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{1\le v<u\le n}\ \sum_{1\le i,t\le n}\left((\eta_{u,v}+\eta_{v,u})\theta_u^{2^{i-1}}\theta_v^{2^{t-1}}x^{2^{i-1}+2^{t-1}}\right)+\sum_{u=1}^{n}\mathrm{Tr}(\theta_u x)\eta_{u,u}\\
&= \sum_{1\le t<i\le n}\ \sum_{1\le v<u\le n}\left((\eta_{u,v}+\eta_{v,u})\left(\theta_u^{2^{i-1}}\theta_v^{2^{t-1}}+\theta_u^{2^{t-1}}\theta_v^{2^{i-1}}\right)x^{2^{i-1}+2^{t-1}}\right)+\mathrm{Lin}(x)\\
&= \sum_{1\le t<i\le n}\left(\sum_{1\le u,v\le n}\theta_u^{2^{i-1}}\theta_v^{2^{t-1}}\left(\eta_{v,u}+\eta_{u,v}\right)\right)x^{2^{i-1}+2^{t-1}}+\mathrm{Lin}(x)\\
&= \sum_{1\le t<i\le n} c_{i,t}x^{2^{i-1}+2^{t-1}}+\mathrm{Lin}(x)
\end{aligned}
$$

□

With the help of Lemma 3, the following result can be proved.

Theorem 3 *Let $H=(h_{u,v})\in\mathbb{F}_{2^n}^{n\times n}$ be a symmetric matrix with main diagonal elements all zeros, and L be a linear permutation on $\mathbb{F}_{2^n}$. Let $H'=(h'_{u,v})\in\mathbb{F}_{2^n}^{n\times n}$ such that $h'_{u,v}=L(h_{u,v})$ for all $1\le u,v\le n$. Then the quadratic functions defined by H and H' relative to α are EA-equivalent. In particular, H is a QAM if and only if H' is a QAM.*

Proof Let the corresponding functions of H and H' be $F(x)=\sum_{1\le t<i\le n}c_{i,t}x^{2^{i-1}+2^{t-1}}$ and $F'(x)=\sum_{1\le t<i\le n}c'_{i,t}x^{2^{i-1}+2^{t-1}}$ respectively.

Let C_F be the same as in Sect. 2. Then $H=M^TC_FM$. Hence $C_F=(M^T)^{-1}HM^{-1}=M_\theta HM_\theta^t$, where θ is the dual basis of α, see Sect. 2.1. So

$$c_{i,t}=\sum_{1\le u,v\le n}\theta_u^{2^{i-1}}\theta_v^{2^{t-1}}h_{u,v}.$$

Choose $\eta_{u,v}\in\mathbb{F}_{2^n}$ such that $\eta_{u,v}+\eta_{v,u}=h_{u,v}$ for all $1\le u,v\le n$, and let $\eta_{u,u}=0$ for all $1\le u\le n$. Define a quadratic function $Q(x)$ over $\mathbb{F}_{2^n}$ as follows:

$$
\begin{aligned}
Q(x)&=\sum_{1\le v<u\le n}\mathrm{Tr}(\theta_u x)\mathrm{Tr}(\theta_v x)h_{u,v}\\
&=\sum_{1\le v<u\le n}\mathrm{Tr}(\theta_u x)\mathrm{Tr}(\theta_v x)(\eta_{u,v}+\eta_{v,u}).
\end{aligned}
$$

Then from the proof of Lemma 3, we have

$$Q(x)=F(x)+\mathrm{Lin}(x), \tag{8}$$

for some linear function $\mathrm{Lin}(x)$ over $\mathbb{F}_{2^n}$.

Furthermore we define $Q'(x)$ by

$$Q'(x)=\sum_{1\le v<u\le n}\mathrm{Tr}(\theta_u x)\mathrm{Tr}(\theta_v x)h'_{u,v}. \tag{9}$$

Using the same reasoning as $Q(x)$ and $F(x)$, we get $Q'(x)=F'(x)+\mathrm{Lin}'(x)$ for some linear function $\mathrm{Lin}'(x)$ over $\mathbb{F}_{2^n}$.

Thus we have

$$\begin{aligned}
Q'(x) &= \sum_{1\le v<u\le n} \mathrm{Tr}(\theta_u x)\mathrm{Tr}(\theta_v x)h'_{u,v} \\
&= \sum_{1\le v<u\le n} \mathrm{Tr}(\theta_u x)\mathrm{Tr}(\theta_v x)L(h_{u,v}) \\
&= L\left(\sum_{1\le v<u\le n} \mathrm{Tr}(\theta_u x)\mathrm{Tr}(\theta_v x)h_{u,v}\right) \\
&= L(Q(x)). \qquad (10)
\end{aligned}$$

By (8), (9) and (10), it deduces that $F(x)$ and $F'(x)$ are EA-equivalent. □

Remark 1 Let $H = (h_{u,v})_{n\times n}$ and $H' = (h'_{u,v})_{n\times n}$ be two $n \times n$ matrices, and L be a linear permutation on $\mathbb{F}_{2^n}$, then $H' = L(H)$ means that $h'_{u,v} = L(h_{u,v})$ for all $1 \le u, v \le n$.

Based on Theorem 2 and Theorem 3 we can obtain the following corollaries.

Corollary 1 *Let $F(x)$ and $F'(x)$ be two quadratic homogeneous functions, and H and H' be their corresponding matrices, respectively. Then $F(x)$ is EA-equivalent to $F'(x)$ if $H' = L(P^t HP)$, where P is an $n\times n$ invertible matrix over $\mathbb{F}_2$, and L is a linear permutation over $\mathbb{F}_{2^n}$.*

Remark 2 Let $F(x)$ and $F'(x)$ be two quadratic homogeneous functions, and H and H' be their corresponding matrices, respectively. We refer to [18,19] for a characterization for EA-equivalence of F and F'.

Up to now, we have introduced the main theoretical results of the paper which are the theoretical bases of Algorithm 1 in the next section.

4 Constructing quadratic APN functions from a given QAM

In this section, we will give an algorithm to construct QAMs, from which we can get lots of new quadratic APN functions. Our algorithm can be summarized as guess and determine, which means we modify the elements of a known QAM to get a new matrix, and then determine whether the new matrix is a QAM. With the help of previous results, the data complexity of constructing new quadratic APN functions can be greatly reduced.

4.1 Properties of matrices over $\mathbb{F}_{2^n}$

In this subsection, we will give several results on matrices over $\mathbb{F}_{2^n}$ which are useful for designing effective algorithms for constructing quadratic APN functions.

Lemma 4 *Let $H \in \mathbb{F}_{2^n}^{n\times n}$ be a symmetric matrix with main diagonal elements all zero. Then every nonzero linear combination over $\mathbb{F}_2$ of the n rows of H has rank at most $n-1$.*

Proof Obviously, $H[i]$ has rank at most $n-1$ for any $1 \le i \le n$. Suppose $\mu = H[i_1] + H[i_2] + \cdots + H[i_t]$, where $2 \le t \le n$ and $\{i_1, i_2, \ldots, i_t\}$ is a subset of $\{1, 2, \ldots, n\}$. Then we have $\mu[i_1] + \mu[i_2] + \cdots + \mu[i_t] = 0$, so $\mathrm{Rank}_{\mathbb{F}_2}(\mu) \le \mathrm{n} - 1$, which implies this proposition. □

For the convenience of our discussions, we give the following definition:

Definition 6 Let $H \in \mathbb{F}_{2^n}^{m \times k}$ $(m, k \leq n)$. H is called proper if every nonzero linear combination over $\mathbb{F}_2$ of the m rows of H has rank at least $k-1$.

First, we give the following lemma.

Lemma 5 *Let $A \in \mathbb{F}_{2^n}^{r \times c}$ $(1 \leq r < c \leq n)$, and $A' = AP$, where $P \in \mathbb{F}_2^{c \times c}$ is invertible. Then A is proper implies that A' is also proper.*

Proof Let $S = \{\sum_{i=1}^{r} \lambda_i A[i] : (\lambda_1, \ldots, \lambda_r) \in \mathbb{F}_2^r \backslash \{0\}\}$, and $S' = \{\sum_{i=1}^{r} \lambda_i A'[i] : (\lambda_1, \ldots, \lambda_r) \in \mathbb{F}_2^r \backslash \{0\}$. Let $S'' = \{sP : s \in S\}$. Then $S' = S''$, and since P is invertible, we have $\text{Rank}_{\mathbb{F}_2}(s) = \text{Rank}_{\mathbb{F}_2}(sP)$. □

Now we can prove the following theorem:

Theorem 4 *Let $A = (a_{i,j}) \in \mathbb{F}_{2^n}^{r \times c}$ $(1 \leq r < c \leq n)$ with $a_{i,j} = a_{j,i}$ and $a_{i,i} = 0$ for $1 \leq i, j \leq r$. Let $A[\cdot, k]$ be the k-th column of A, and $b = \sum_{k=1}^{c} \lambda_k A[\cdot, k]$, where $0 \neq (\lambda_1, \ldots, \lambda_c) \in \mathbb{F}_2^c$. Assume $t = \text{Rank}_{\mathbb{F}_2}\{b[1], b[2], \ldots, b[r]\}$. If A is proper, then we have:*
(i) If $(\lambda_{r+1}, \ldots, \lambda_c) = 0$, then $t = r - 1$;
(ii) If $(\lambda_{r+1}, \ldots, \lambda_c) \neq 0$, then $t = r$.

Proof (i) Assume $(\lambda_{r+1}, \ldots, \lambda_c) = 0$. Then $b = \sum_{k=1}^{r} \lambda_k A[\cdot, k]$. By Lemma 4, $t \leq r - 1$. Let $B = \text{Submatrix}(A, 1, 1, r, r)$, by the definition of A, we have

$$\text{Rank}_{\mathbb{F}_2}\left(\sum_{k=1}^{r} \lambda_k A[\cdot, k]\right) = \text{Rank}_{\mathbb{F}_2}\left(\sum_{k=1}^{r} \lambda_k B[\cdot, k]\right)$$
$$= \text{Rank}_{\mathbb{F}_2}\left(\sum_{k=1}^{r} \lambda_k B[k]\right).$$

If $t < r - 1$, then we have $\text{Rank}_{\mathbb{F}_2}(\sum_{k=1}^{r} \lambda_k A[k]) < r - 1 + (c - r) = c - 1$, which contradicts with A being proper. Thus $t = r - 1$.

(ii) Suppose $(\lambda_{r+1}, \ldots, \lambda_c) \neq 0$. Without loss of generality, let $\lambda_c = 1$. Then substitute $A[\cdot, c]$ with b, we get a new $r \times c$ matrix A'. If $t < r$, then there exists $0 \neq (\lambda_1', \ldots, \lambda_r') \in \mathbb{F}_2^r$ such that $\lambda_1' A'[1, c] + \lambda_2' A'[2, c] + \cdots + \lambda_r' A'[r, c] = 0$. Without loss of generality, suppose $\lambda_1' \neq 0$. Next we perform the following operations step by step, first, substitute $A'[1]$ with $\sum_{i=1}^{r} \lambda_i' A'[i]$ and get a new matrix A''; second, substitute $A''[\cdot, 1]$ with $\sum_{i=1}^{r} \lambda_i' A''[\cdot, i]$ and get a new matrix A'''. By Lemma 5 and the definition of the proper, it implies that A', A'' and A''' are also proper. However, after these changes, we have $A'''[1, 1] = A'''[1, c] = 0$, which contradicts with A''' being proper. Thus $t < r$ is not true, so $t = r$. □

According to Theorem 4, we get the following corollary.

Corollary 2 *Let $H = (h_{u,v})_{n \times n}$ be an $n \times n$ symmetric matrix over $\mathbb{F}_{2^n}$, and $A = \text{Submatrix}(H, 1, 1, r, c)$ with $r < c$. Suppose $B = A^T = \text{Submatrix}(H, 1, 1, c, r)$. Then A is proper implies that B is also proper.*

Corollary 2 will be useful to speed up our algorithm for constructing QAMs. The key point is that every submatrix of a QAM must be proper (see Definition 6), so if a matrix has a submatrix which is not proper, it cannot be a QAM. Based on this corollary, we can exclude some improper candidates in advance when we haven't known the whole values of the matrix. We know that every QAM is symmetric, so we will know the values of $A = \mathrm{Submatrix}(H, 1, 1, r, c)$ and $B = A^T = \mathrm{Submatrix}(H, 1, 1, c, r)$ at the same time. According to Corollary 2, we need only to check whether A is proper. Thus some unnecessary checking can be avoided in our searching algorithm.

4.2 How to construct QAMs

In this section, we will introduce a problem, and then show how to construct QAMs through solving this problem.

Problem 1 *Let e_i be a vector of length n with $e_i[i] = 1$ and $e_i[j] = 0$ for $j \neq i$. The problem is, how to find $\overrightarrow{x} = (x_1, \ldots, x_{n-1}) \in \mathbb{F}_{2^n}^{n-1}$ satisfying*

$$\lambda_1 x_1 + \cdots + \lambda_{n-1} x_{n-1} \in S_{\lambda_1 e_1 + \cdots + \lambda_{n-1} e_{n-1}}, \tag{11}$$

for all $(\lambda_1, \ldots, \lambda_{n-1}) \in \mathbb{F}_2^{n-1} \backslash \{0\}$, where $S_{\lambda_1 e_1 + \cdots + \lambda_{n-1} e_{n-1}}$ are some subsets of $\mathbb{F}_{2^n}$.

(11) consists of $2^{n-1} - 1$ conditions, we need to find all the qualified $\overrightarrow{x}$. As a matter of fact, all the constructions of QAMs can be reduced to Problem 1. Details are described as follows.

Given an $n \times n$ QAM matrix H over $\mathbb{F}_{2^n}$, we wish to reassign the values of the last column of H to get some new QAMs. Let $A = \mathrm{Submatrix}(H, 1, 1, n-1, n-1)$, it is easy to see that A is proper. By Lemma 4, any nonzero linear combination of the $n-1$ rows of A has rank $n-2$.

Let $c = (x_1, \ldots, x_{n-1})^t$, and $H' = \begin{pmatrix} A & c \\ c^t & 0 \end{pmatrix}$. We want to choose suitable c to make H' a QAM. Actually, by Theorem 4 (ii), we need only to choose $c = (x_1, \ldots, x_{n-1})^t$ to satisfy (11), where $S_{\lambda_1 e_1 + \cdots + \lambda_{n-1} e_{n-1}} = \mathbb{F}_{2^n} \backslash \mathrm{Span}(\lambda_1 A[1] + \cdots + \lambda_{n-1} A[n-1])$.

We can shrink S_{e_1} in (11). Let $V = \mathrm{Span}(A[1,1], A[1,2], \ldots, A[1, n-1])$, in (11), $S_{e_1} = \mathbb{F}_{2^n} \backslash V$, which equals to $(V + a_1) \cup (V + a_2) \cup (V + a_3)$ for some $a_i \in \mathbb{F}_{2^n}$, $1 \leq i \leq 3$ because of $\dim(V) = n-2$. Since $x_1 \in S_{e_1}$, there exists $y \in V$ such that $x_1 = y + a_i$ for some i, i.e., $a_i = x_1 + y$. Since $y \in V$ and $A[1,1] = 0$, $y = \lambda_2 A[1,2] + \cdots + \lambda_{n-1} A[1, n-1]$ for some $\lambda_i \in \mathbb{F}_2$, $i = 2, \ldots, n-1$. So we may perform suitable column transformations to change x_1 into a_i, and perform the corresponding row transformations to change $H'[n, 1]$ into a_i. Since we consider only to find CCZ-inequivalent functions, so by Theorem 2, we may take $S_{e_1} = \{a_1, a_2, a_3\}$. Because in the above transformation, we do not use the first column, therefore based on the same reason as the S_{e_1}, we may take $S_{e_2} = \{b_1, \ldots, b_l\}$, where $l = 2^{n-1} - 2^{n-3}$.

Further, given a QAM H, we may also reassign the values of the last two columns of H to get some new QAMs. This can also be reduced to Problem 1, the difference is that we must apply the problem twice. Similarly, we can reassign more columns of H, so this method can generate almost all CCZ-inequivalent quadratic APN functions if we change enough columns.

In view of the above discussions, an algorithm for solving Problem 1 is important for our approach for constructing new quadratic functions. We give a recursive algorithm as Algorithm 1. It needs to run GenerateQAM$(1, H, S)$ to solve Problem 1.

In the following, we give an example to illustrate the above algorithm.

Example 1 Let $n = 4$ and we work on $\mathbb{F}_{2^4}$, and

$$H = \begin{pmatrix} 0 & H[1,2] & H[1,3] & \mathbf{x_1} \\ H[2,1] & 0 & H[2,3] & \mathbf{x_2} \\ H[3,1] & H[3,2] & 0 & \mathbf{x_3} \\ \mathbf{x_1} & \mathbf{x_2} & \mathbf{x_3} & 0 \end{pmatrix}.$$

Suppose A = Submartix(H, 1, 1, 3, 3) is proper. The above algorithm is about how to keep H proper when assigning values for x_1, x_2 and x_3. The basic idea is, if $x_1 \in \mathrm{Span}(A[1])$, then H is not proper. So x_1 must be chosen such that $x_1 \in \mathbb{F}_{2^4} \backslash \mathrm{Span}(A[1])$. Similarly, if $x_1 + x_2 \in \mathrm{Span}(A[1] + A[2])$, then H is not proper, thus $x_1 + x_2 \in \mathbb{F}_{2^4} \backslash \mathrm{Span}(A[1] + A[2])$. With the same reasoning, H is proper if and only if

```
$A \leftarrow$ Submatrix$(H, 1, 1, n-1, n-1)$;
$e_t \in \mathbb{F}_2^{n-1}$ with $e_t[t] = 1$ and $e_t[j] = 0$ for $j \neq t$;
for each $(\lambda_1, \lambda_2, \ldots, \lambda_{n-1}) \in \mathbb{F}_2^{n-1} \backslash \{0\}$ do
    $S_{(\lambda_1,\ldots,\lambda_{n-1})} \leftarrow \mathbb{F}_{2^n} \backslash \mathrm{Span}(\sum_{j=1}^{n-1} \lambda_j A[j])$;
end
$S = \{S_\lambda : \lambda = (\lambda_1, \cdots, \lambda_{n-1}) \in \mathbb{F}_2^{n-1} \backslash \{0\}\}$;
Input: A QAM $H$ over $\mathbb{F}_{2^n}$; A set $S$ as defined above; An index $i$.
Output: Some QAMs;
procedure GenerateQAM($i$, $H$, $S$);
if $i = n - 1$ then
    for each $x_i \in S_{e_i}$ do
        $H[n, n-1] \leftarrow x_i$;
        $H[n-1, n] \leftarrow x_i$;
        Output H;
    end
else
    for each $x_i \in S_{e_i}$ do
        $H[n, i] \leftarrow x_i$;
        $H[i, n] \leftarrow x_i$;
        $S' \leftarrow S$;
        for each $(\lambda_{i+1}, \ldots, \lambda_{n-1}) \in \mathbb{F}_2^{n-1-i} \setminus \{0\}$ do
            $\lambda \leftarrow (0, \ldots, 0, \lambda_{i+1}, \ldots, \lambda_{n-1})$;
            $S'_\lambda \leftarrow S_\lambda \cap S_{\lambda \oplus e_i}$;
            GenerateQAM($i + 1$, $H$, $S'$);
        end
    end
end
end procedure
```

Algorithm 1: An algorithm for solving Problem 1

$$\begin{cases} x_1 \in \mathbb{F}_{2^4} \backslash \mathrm{Span}(A[1]), \\ x_2 \in \mathbb{F}_{2^4} \backslash \mathrm{Span}(A[2]), \\ x_3 \in \mathbb{F}_{2^4} \backslash \mathrm{Span}(A[3]), \\ x_1 + x_2 \in \mathbb{F}_{2^4} \backslash \mathrm{Span}(A[1] + A[2]), \\ x_1 + x_3 \in \mathbb{F}_{2^4} \backslash \mathrm{Span}(A[1] + A[3]), \\ x_2 + x_3 \in \mathbb{F}_{2^4} \backslash \mathrm{Span}(A[2] + A[3]), \\ x_1 + x_2 + x_3 \in \mathbb{F}_{2^4} \backslash \mathrm{Span}(A[1] + A[2] + A[3]). \end{cases}$$

The above algorithm is a generalization of this example.

4.3 Experimental results

We have implemented the algorithm of this paper. In this subsection we will report experimental results running our algorithm.

(i) Dillon [13] listed 18 classes of CCZ-inequivalent APN functions over $\mathbb{F}_{2^7}$. Edel [16] found a new class of APN function and this list expanded to 19 classes. With the method of this paper, firstly, we construct a 7×7 QAM H from x^3, then reassign the values $H[3, 6]$, $H[3, 7]$, $H[4, 5]$, $H[4, 6]$, $H[4, 7]$, $H[5, 6]$, $H[5, 7]$ and $H[6, 7]$ (during this process, we must keep H symmetric). Using this idea we can get more than 470 classes of CCZ-inequivalent quadratic APN functions, these functions are all CCZ-inequivalent to the known ones. Similar method can be used on $\mathbb{F}_{2^6}$. According to Edel's results [15], there is only 13 classes of CCZ-inequivalent quadratic APN functions on $\mathbb{F}_{2^6}$. Our algorithm shows that we need only to change 8 (2×4) elements of of a QAM and get all 13 classes of CCZ-inequivalent quadratic APN functions.

(ii) We must change the last two columns (and rows) of a known QAM to get new QAMs when $n \geq 8$. On $\mathbb{F}_{2^8}$, it needs about 24 h to find a new APN function in a personal computer. Fortunately, Algorithm 1 can be implemented in parallel, and we are running our programs in several computers now. Up to know, we have found about 2252 CCZ-inequivalent quadratic APN functions on $\mathbb{F}_{2^8}$, and they are all CCZ-inequivalent to the 23 classes of known ones introduced by Dillon [13] and Edel and Pott [16]. We have checked all these new APN functions with the method introduced in [5], none of them is CCZ-equivalent to a permutation. We refer the readers to [25] for detailed experimental results, where we list all newly found APN functions in polynomial forms.

5 Conclusion

A one to one correspondence between quadratic homogeneous APN functions and QAMs is presented. In view of this correspondence, we propose the notion of the proper for matrices over a finite field. The most important part of our algorithm is how to keep the matrix proper during the construction process. Algorithm 1 is the core part of our searching program.

Up to now, we have found 471 and 2252 new CCZ-inequivalent quadratic APN functions on $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$ respectively (see the appendices in [25]). We think our lists are not complete, especially the list on $\mathbb{F}_{2^8}$. Much related work can be done in the future, such as, finding some QAMs whose corresponding functions are APN on $\mathbb{F}_{2^n}$ for infinitely many n, generalizing the matrix approach to construct PN functions, and finding better methods to construct QAMs, etc.

Acknowledgments The authors thank Yves Edel for the early discussion about how to check the CCZ-equivalence between APN functions. Moreover the authors are very grateful to referees for their valuable comments on this paper which have greatly improved the presentation of the paper. This work was supported in part by 973 project under Grant (2013CB834203), and by the National Science Foundation of China under Grand (61379142, 61303255).

References

1. Beth T., Ding C.: On almost perfect nonlinear permutations. In: Advances in Cryptology—EUROCRYPT'93. LNCS, vol. 765, pp. 65–76. Springer, New York (1994).
2. Bracken C., Byrne E., Markin N., McGuire G.: New families of quadratic almost perfect nonlinear trinomials and multinomials. Finite Fields Appl. **14**(3), 703–714 (2008).
3. Bracken C., Byrne E., Markin N., McGuire G.: A few more quadratic APN functions. Cryptogr. Commun. **3**(3), 43–53 (2011).
4. Browning K., Dillon J.F., McQuistan M.: APN polynomials and related codes. J. Comb. Inf. Syst. Sci., **34**(1–4), 135–159, (2009) (Special volume honoring the 75-th birthday of Prof. D.K.Ray-Chaudhuri).
5. Browning K., Dillon J.F., McQuistan M., Wolfe A.J.: An APN permutation in dimension six. Contemaray Math. **58**, 33–42 (2010).
6. Budaghyan L., Carlet C., Pott A.: New classes of almost bent and almost perfect nonlinear polynomials. IEEE Trans. Inf. Theory **52**(3), 1141–1152 (2006).
7. Budaghyan L., Carlet C.: Classes of quadratic APN trinomials and hexanomials and related structures. IEEE Trans. Inf. Theory **54**(5), 2354–2357 (2008).
8. Budaghyan L, Carlet C., Leander G.: Constructing new APN functions from known ones. Finite Fields Appl. **15**(2), 150–159 (2009).
9. Budaghyan L., Carlet C., Leander G.: Two classes of quadratic APN binomials inequivalent to power functions. IEEE Trans. Inf. Theory **54**(9), 4218–4229 (2008).
10. Carlet C.: Vectorial Boolean functions for cryptography, In: Crama Y., Hammer P. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 398–469. Cambridge University Press, Cambridge. http://www.math.univ-paris13.fr/~carlet/pubs.html (2014). Accessed 25 Aug 2013.
11. Carlet C., Charpin P., Zinoviev V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. **15**(2), 125–156 (1998).
12. Daemen J., Rijmen V.: The Design of Rijndael. Springer (2002).
13. Dillon J.F.: APN polynomials: an update, Fq9, In: The 9th International Conference on Finite Fields and Their Applications, Dublin (2009).
14. Edel Y.: Geoemetric and combinatorial aspects of APN functions. In: Contact Forum: Coding Theory and Cryptography III, Brussels. http://cage.ugent.be/~ls/website2009/abstracts/slidesyvesedel.pdf (2009). Accessed 20 Aug 2013.
15. Edel Y.: Quadratic APN functions as subspaces of alternating bilinear forms. In: Proceedings of the Contact Forum Coding Theory and Cryptography III, Belgium 2009, pp. 11–24 (2011).
16. Edel Y., Pott A.: A new almost perfect nonlinear function which is not quadratic. Adv. Math. Commun. **3**(1), 59–81 (2009).
17. Edel Y., Kyureghyan G., Pott A.: A new APN function which is not equivalent to a power mapping. IEEE Trans. Inf. Theory **52**(2), 744–747 (2006).
18. Dempwolff U., Edel Y.: Dimensional dual hyperovals and APN functions with translation group. J. Algebr. Comb. **39**, 457–496. http://link.springer.com/article/10.1007 (2014).
19. Edel Y.: On quadratic APN functions and dimensional dual hyperovals. Des. Codes Cryptogr. **57**(1), 35–44 (2010).
20. Gold R.: Maximal recursive sequences with 3-valued recursive cross-correlation functions. IEEE Trans. Inf. Theory **14**(1), 154–156 (1968).
21. Lidl R., Niederreiter H.: Finite Fields, pp. 58. Cambridge University Press, Cambridge (1983).
22. Ling S., Qu L.J.: A note on linearized polynomials and the dimension of their kernels. Finite Fields Appl. **18**(1), 56–62 (2012).
23. Nyberg K., Knudsen L.R.: Provable security against differential cryptanalysis. In: CRYPTO 92. LCNS, vol. 740, pp. 566–574. Springer, New York (1993).
24. Yoshiara S.: Equivalences of quadratic APN functions. J. Algebr. Comb. **35**(3), 461–475 (2012).
25. Yu Y., Wang M., Li Y.: A matrix approach for constructing quadratic APN functions. Cryptology ePrint Archive. Report (2013/2007).