Classification of quadratic APN functions with coefficients in $\mathbb{F}_2$ for dimensions up to 9

Yuyin Yu[1] Nikolay Kaleyski[2] Lilya Budaghyan[2]
Yongqiang Li[3]

December 28, 2019

Abstract

Almost perfect nonlinear (APN) and almost bent (AB) functions are integral components of modern block ciphers and play a fundamental role in symmetric cryptography. In this paper, we describe a procedure for searching for quadratic APN functions with coefficients in $\mathbb{F}_2$ over the finite fields $\mathbb{F}_{2^n}$ and apply this procedure to classify all such functions over $\mathbb{F}_{2^n}$ with $n \leq 9$. We discover two new APN functions (which are also AB) over $\mathbb{F}_{2^9}$ that are CCZ-inequivalent to any known APN function over this field. We also verify that there are no quadratic APN functions with coefficients in $\mathbb{F}_2$ over $\mathbb{F}_{2^n}$ with $6 \leq n \leq 8$ other than the currently known ones.

1 Introduction

A vectorial Boolean (n, m)-function is a function between the vector spaces $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$ over the finite field $\mathbb{F}_2 = \{0, 1\}$ for some two positive integer m, n. Vectorial Boolean functions play a crucial role in the design of modern block ciphers (where they are referred to as "S-boxes" or "substitution boxes"), in which they typically represent the only non-linear part of the encryption. For this reason, the resistance of a block cipher to cryptanalytic attacks directly depends on the properties of its substitution boxes. Vectorial Boolean (n, n)-functions are of particular importance in cryptography since one typically wishes to substitute a sequence of bits for another sequence of the same length. In this case, the vector space $\mathbb{F}_2^n$ is usually identified with the finite field $\mathbb{F}_{2^n}$, and (n, n)-functions are expressed as polynomials over $\mathbb{F}_{2^n}$.

1. College of Mathematics and Information Science, Guangzhou University, Guangzhou (yuyuyin@163.com)
2. Department of informatics, University of Bergen (Lilya.Budaghyan@uib.no, Nikolay.Kaleyski@uib.no); the research of the second and the third author is supported by the "Optimal Boolean functions" grant of the Trond Mohn foundation
3. State Key Laboratory of Information Security,Institute of Information Engineering, Chinese Academy of Sciences (yongq.lee@gmail.com)

Among the most powerful cryptanalytic attacks known to date are the so-called "differential cryptanalysis" introduced by Biham and Shamir [1] and "linear cryptanalysis" introduced by Matsui [24]. Almost perfect nonlinear (APN) functions were introduced by Nyberg [25] as the class of (n, n)-functions offering optimal resistance to differential cryptanalysis, while almost bent (AB) functions are the ones that are optimal against linear cryptanalysis [20]. Finding new examples and constructions of APN and AB functions is very important not only for the purpose of constructing new block ciphers in cryptography, but for other areas of computer science and discrete mathematics (such as combinatorics, sequence design, coding theory, design theory) in which APN functions correspond to some optimal objects. Furthermore, finding new APN and AB functions is a difficult task, especially for large dimensions n: indeed, to date only six infinite monomial APN families and twelve infinite polynomial APN families have been discovered [1], despite ongoing research on the topic since the early 90's. Among these, there are four infinite families of AB monomials and eight infinite families of AB polynomials.

The case of quadratic APN functions is more tractable than the general one, which is evinced by the fact that all the infinite polynomial families constructed so far are quadratic, and only one known sporadic example of a non-quadratic (up to CCZ-equivalence) APN function (which is defined over $\mathbb{F}_{2^6}$) is known [22]. Nevertheless, quadratic APN functions are an important ongoing direction of research: in 2010, Dillon et al. discovered an APN permutation in dimension $n = 6$, thereby disproving the conjecture that APN functions over fields of even dimension could never be bijective [5]. Despite Dillon's permutation not being a quadratic APN function per se, it was constructed by traversing the CCZ-equivalence class of a quadratic function. The question of the existence of other APN permutations for even n remains open, and investigating new instances of quadratic APN functions is a promising way to approach it.

A lot of research has been done on the topic of APN functions in recent years. An infinite construction of APN binomials inequivalent to power functions is given in [12], disproving the long-standing conjecture that all infinite APN families must be monomials. Further infinite constructions of APN and AB functions are proposed in [7, 8, 9, 10, 11, 12, 13, 14, 2, 28, 26]. Previously, a classification of all APN functions over $\mathbb{F}_{2^n}$ for n up to 5 was given in [3], with classification for dimensions n higher than 5 remaining incomplete at the time of writing. In the case of $n = 6$, classification is complete for the particular cases of quadratic and cubic functions: in [4], 13 CCZ-inequivalent quadratic functions over $\mathbb{F}_{2^6}$ are listed, and it is shown that these encompass all quadratic CCZ-classes over $\mathbb{F}_{2^6}$ in [21]; as for the case of cubic APN functions, their classification is given in [23]. Furthermore, a study of the EA-equivalence classes corresponding to all known APN functions over $\mathbb{F}_{2^6}$ is presented in [16, 17]. More background on APN functions and their construction can be found e.g. in [6] or [18].

[1] Tables of the known infinite monomial and polynomial families can be found at https://boolean.h.uib.no/mediawiki/

Using a matrix construction, a large number of CCZ-inequivalent APN functions were found over $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$ [27], bringing the total number of known APN functions to 490 and 8180, respectively. To the best of our knowledge, no systematic search of this kind has been performed over $\mathbb{F}_{2^n}$ for any dimension $n \geq 9$. The main reason for this is that the complexity of a computer search (which increases exponentially with the dimension n) becomes too demanding over dimensions of this magnitude. In this paper, we focus on the particular case of quadratic APN functions over $\mathbb{F}_{2^n}$ with $n \leq 9$ and with coefficients in $\mathbb{F}_2$. We employ a specialization of the matrix method presented in [27] to conduct our search, and obtain a complete classification (up to CCZ-equivalence) of these functions over $\mathbb{F}_{2^9}$. In particular, we discover two instances of APN functions over $\mathbb{F}_{2^9}$ that are inequivalent to any known APN function over this field. For dimensions n with $6 \leq n \leq 8$, this proves that there are no other quadratic APN functions with coefficients in $\mathbb{F}_2$ than the already known ones.

In our classification, we list the shortest possible representatives from each CCZ-equivalence class that we have found. In dimensions n up to 6, these shortest representatives are all monomials. In dimensions $n \in \{7, 8\}$, the longest representative has 6 terms, while in dimension $n = 9$, the longest representative has 9 terms. This raises the question of whether any quadratic APN function over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_2$ can be represented by a polynomial with at most n terms.

Furthermore, although all of the functions that we find over $\mathbb{F}_{2^8}$ are equivalent to representatives from [22], we find shorter representatives for two of these functions, viz. $x^3 + x^6 + x^{72}$ for $x^3 + \mathrm{Tr}(x^9)$ and $x^3 + x^6 + x^{144}$ for $x^9 + \mathrm{Tr}(x^3)$. Thus, to the best of our knowledge, our classification lists the shortest known representatives for the CCZ-equivalence classes in question.

2 Preliminaries

Let n be a positive integer. We denote by $\mathbb{F}_{2^n}$ the finite field with 2^n elements, by $\mathbb{F}_{2^n}^\star$ its multiplicative group, and by $\mathbb{F}_{2^n}[x]$ the univariate polynomial ring over $\mathbb{F}_{2^n}$ in indeterminate x. By $\mathbb{F}_{2^n}^{m\times k}$ we denote the set of m-by-k matrices with entries in $\mathbb{F}_{2^n}$, and if $M \in \mathbb{F}_{2^n}^{m\times k}$, we denote by $M[i, j]$ the entry in the i-th row and j-th column of M, for $0 \leq i \leq m-1$, $0 \leq j \leq k-1$. Note that we index matrix rows and columns from zero.

We will use the following conventions and notation throughout the paper:

(i) Suppose $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ is a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, so that $\alpha_{i+1} = \alpha_i^2$ for $0 \leq i \leq n-1$, and suppose $\{\theta_0, \theta_1, \ldots, \theta_{n-1}\}$ is its dual basis, i.e. $\mathrm{Tr}(\alpha_i\theta_j) = 0$ for $i \neq j$ and $\mathrm{Tr}(\alpha_i\theta_i) = 1$ for $0 \leq i, j \leq n-1$. Note that $\{\theta_0, \theta_1, \ldots, \theta_{n-1}\}$ is also a normal basis, so that without loss generality we can assume $\theta_{i+1} = \theta_i^2$ for $0 \leq i \leq n-1$.

Let $M_\alpha \in \mathbb{F}_{2^n}^{n\times n}$ and $M_\theta \in \mathbb{F}_{2^n}^{n\times n}$ be such that

$$M_\alpha[i, u] = \alpha_u^{2^i} \text{ and } M_\theta[i, u] = \theta_u^{2^i} \tag{1}$$

for $0 \leq u, i \leq n-1$. Then $M_\alpha^t M_\theta[u,j] = \mathrm{Tr}(\alpha_u \theta_j)$ for $0 \leq u, j \leq n-1$, so that $M_\alpha^t M_\theta = I_n$, where I_n is the identity matrix of order n. Thus $M_\theta^{-1} = M_\alpha^t$, where M_α^t is the transpose of M_α.

(ii) Let $B \in \mathbb{F}_{2^n}^m$ be the vector $B = (\eta_0, \eta_1, \cdots \eta_{m-1})$ where $\eta_i \in \mathbb{F}_{2^n}$ for $0 \leq i \leq m-1$. Then $\mathrm{Span}(B) = \mathrm{Span}(\eta_0, \eta_1, \cdots, \eta_{m-1})$ is the sub-space spanned by $\{\eta_0, \eta_1, \cdots, \eta_{m-1}\}$ over $\mathbb{F}_2$. The dimension of this subspace is denoted by $\mathrm{Rank}(B) = \mathrm{Rank}(\eta_0, \eta_1, \cdots, \eta_{m-1})$, and is referred to as the rank of B over $\mathbb{F}_2$.

If $\eta_i = \sum_{j=0}^{n-1} \lambda_{i,j} \alpha_j$ for $0 \leq j \leq m-1$, with $\lambda_{i,j} \in \mathbb{F}_2$ for $0 \leq i, j \leq n-1$, and we define an m-by-n matrix $\Lambda \in \mathbb{F}_2^{m \times n}$ by $\Lambda[i,j] = \lambda_{i,j}$, then the rank of B is equal to the rank of Λ.

An (n,n)-function, or vectorial Boolean function, is any mapping $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ from the field with 2^n elements to itself. Any (n,n)-function can be represented as a polynomial $F(x) = \sum_{i=0}^{2^n-2} a_i x^i$ over $\mathbb{F}_{2^n}$ with $a_i \in \mathbb{F}_{2^n}$; this representation is referred to as the univariate representation of F, and is unique. The binary weight $wt_2(i)$ of a positive integer i is the number of ones in its binary notation; equivalently, if we write i as a sum of powers of two, so that $i = \sum_{j=0}^{k} b_j 2^j$ for $b_j \in \{0,1\}$, then its binary weight is $wt_2(x) = \sum_{i=0}^{k} b_j$, with the sum taken over the integers. The largest binary weight of an exponent i in the univariate representation of an (n,n)-function F with non-zero coefficient a_i is called the algebraic degree of F and is denoted by $\deg(F)$. A function of algebraic degree 1, resp. 2, resp. 3 is called affine, resp. quadratic, resp. cubic. An affine F satisfying $F(0) = 0$ is called linear.

In the following, we concentrate on the case of homogeneous quadratic functions, which can be written as

$$F(x) = \sum_{0 \leq i < j \leq n-1} a_{i,j} x^{2^i + 2^j}$$

for $a_{i,j} \in \mathbb{F}_{2^n}$, i.e. quadratic functions with no linear terms in their univariate representation.

Definition 1. *A mapping $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ 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)**.*

Definition 2. *Let F and F' be two functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. We say that F and F' are **EA-equivalent** (Extended affine equivalent) if we can write F' as*

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

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

*We say that F and F' are **CCZ-equivalent** (Carlet-Charpin-Zinoviev equivalent) [19], 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'.*

EA-equivalence is a special case of CCZ-equivalence, and the latter, which also includes taking inverses of permutations as a particular case, is known to be strictly more general that the combination of both of the aforementioned transformations. An important property of CCZ-equivalence is that it leaves the differential uniformity $\delta(F)$ invariant, i.e. if two (n, n)-functions F and F' are CCZ-equivalent, then $\delta(F) = \delta(F')$. For this reason, APN functions are typically classified up to CCZ-equivalence, and this makes the classification process somewhat easier despite the large amount of (n, n)-functions.

Definition 3. *Let $H \in \mathbb{F}_{2^n}^{m\times k}$ $(m, k \leq n)$. We say that H is **proper** if every nonzero linear combination over $\mathbb{F}_2$ of the m rows of H has rank at least $k - 1$.*

Definition 4. *Let $H = (h_{u,v})_{n\times n}$ be an $n \times n$ matrix defined on $\mathbb{F}_{2^n}$. Then H is called a **QAM** (quadratic APN matrix) if:*
i) H is symmetric and the elements in its main diagonal are all zeros;
ii) Every nonzero linear combination of the n rows (or, equivalently, columns due to H being symmetric) of H has rank $n - 1$.

3 Construction of quadratic APN functions

3.1 Correspondence between quadratic functions with coefficients in $\mathbb{F}_2$ and a class of matrices

In our work, we search for new quadratic APN functions by constructing instances of a particular class of matrices. As shown in [27], there is a one-to-one correspondence between quadratic APN functions and QAM's. The precise statement is given in Theorem 1 below.

Theorem 1. *[27] Let $F(x) = \sum_{0\leq t<i\leq n-1} c_{i,t}x^{2^i+2^t} \in \mathbb{F}_{2^n}[x]$ be a homogeneous quadratic (n, n)-function and let $C_F \in \mathbb{F}_{2^n}^{n\times n}$ be defined by $C_F[i, t] = C_F[t, i] = c_{i,t}$, $C_F[i, i] = 0$ for $0 \leq i < t \leq n - 1$. Let $H = M_\alpha^t H M_\alpha$ where M_α is as defined in (1). Then $\delta(F) = 2^k$ if and only if any non-zero linear combination of the n rows of H has rank at least $n - k$. In particular, F is APN if and only if H is a QAM.*

The following theorem addresses the specific case when all coefficients of the function (and hence all entries of the matrix) are in $\mathbb{F}_2$.

Theorem 2. *Let $F(x) = \sum\limits_{0\leq t<i\leq n-1} c_{i,t}x^{2^i+2^t}$ be a quadratic homogeneous (n, n)-function. Define an $n \times n$ matrix C_F by $C_F[t, i] = C_F[i, t] = c_{i,t}$ for $0 \leq t <$*

$i \leq n-1$ *and* $C_F[i,i] = 0$ *for* $0 \leq i \leq n-1$. *Finally, take*

$$H = M_\alpha^t C_F M_\alpha.$$

Then $H[u+1, v+1] = H[u,v]^2$ *for* $0 \leq v, u \leq n-1$ *if and only if* $c_{i,t} \in \mathbb{F}_2$ *for* $0 \leq t < i \leq n-1$.

Proof. ($\Leftarrow$) Suppose $c_{i,t} \in \mathbb{F}_2$ for $0 \leq t < i \leq n-1$.

From $H = M_\alpha^t C_F M_\alpha$ we have

$$H[u,v] = \sum_{0 \leq t < i \leq n-1} c_{it}(\alpha_u^{2^i}\alpha_v^{2^t} + \alpha_u^{2^t}\alpha_v^{2^i})(0 \leq v, u \leq n-1).$$

It is easy to see that $H[u+1, v+1] = H[u,v]^2$ for $0 \leq v, u \leq n-1$, since $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ is a normal basis such that $\alpha_{i+1} = \alpha_i^2$ for $0 \leq i \leq n-1$.

($\Rightarrow$) From $H = M_\alpha^t C_F M_\alpha$, we have $C_F = (M_\alpha^t)^{-1} H M_\alpha^{-1} = M_\theta H M_\theta^t$, which means that

$$c_{i,t} = C_F[i,t] = \sum_{0 \leq u,v \leq n-1} (\theta_u^{2^i}\theta_v^{2^t})H[u,v](0 \leq v, u \leq n-1).$$

Since $\theta_{i+1} = \theta_i^2$ for $0 \leq i \leq n-1$, if $H[u+1, v+1] = H[u,v]^2$ for $0 \leq v, u \leq n-1$, then we have

$$c_{i,t} = \sum_{0 \leq k \leq n-1} Tr(\theta_0^{2^i}\theta_{0+k}^{2^t} H[0, 0+k]) \in \mathbb{F}_2.$$

□ □

By the above theorem, if we want to construct quadratic APN functions with coefficients in $\mathbb{F}_2$, we only need to construct QAM's such that $H[u+1, v+1] = H[u,v]^2$ for $0 \leq v, u \leq n-1$. This greatly simplifies the search procedure and makes it possible to search for functions in higher dimensions.

3.2 Conditions on QAM's

Suppose $H \in \mathbb{F}_{2^n}^{n \times n}$, $H[u,u] = 0$, $H[u,v] = H[v,u]$ for $0 \leq u, v \leq n-1$, and $H[u+1, v+1] = H[u,v]^2$ for $0 \leq v, u \leq n-1$. In this section we investigate conditions under which H is a QAM.

Example 1. *To better understand the complexity of the search, we look at the concrete example of a QAM for dimension* $n = 6$. *By Theorem 2, such a matrix must necessarily take the form*

$$H = \begin{pmatrix} 0 & a & b & c & b^{2^4} & a^{2^5} \\ a & 0 & a^2 & b^2 & c^2 & b^{2^5} \\ b & a^2 & 0 & a^{2^2} & b^{2^2} & c^{2^2} \\ c & b^2 & a^{2^2} & 0 & a^{2^3} & b^{2^3} \\ b^{2^4} & c^2 & b^{2^2} & a^{2^3} & 0 & a^{2^4} \\ a^{2^5} & b^{2^5} & c^{2^2} & b^{2^3} & a^{2^4} & 0 \end{pmatrix}$$

for some $a, b, c, \in \mathbb{F}_{2^6}$. Thus, it suffices to go over all triples $(a, b, c) \in \mathbb{F}_{2^6}$ in order to exhaust all possible QAM's corresponding to quadratic polynomials over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_2$. Note that the condition $H[u+1, v+1] = H[u, v]^2$ implies that $c = c^{2^3}$, which further reduces the complexity of the search.

Based on the computational results for dimensions $n \leq 9$, we can observe that any quadratic APN function F_1 with coefficients in $\mathbb{F}_2$ appears to be CCZ-equivalent to a quadratic APN function F_2 with at most n non-zero coefficients in $\mathbb{F}_{2^n}$. It would be interesting to establish whether this is true in general; if so, it would indicate the existence of a simple polynomial form for functions of this type, as well as significantly simplify the complexity of searching for them.

This is closely related to the problem of finding a "simplest" possible polynomial representation for a given (n, n)-function F. A simple representation not only results in a polynomial representation that can be evaluated more efficiently in practice, but facilitates the mathematical analysis of the function in question and its properties.

Problem 1. *Given an (n, n)-function F, find a function G, such that G is CCZ-equivalent to F and has the least possible number of non-zero coefficients.*

The contribution of the following proposition is to reduce the search complexity by discarding QAM's which a priori correspond to equivalent functions. Proposition 1 follows from Theorem 3 of [27], which asserts that if $H \in \mathbb{F}_{2^n}^{n \times n}$ is a symmetric matrix, and $H' \in \mathbb{F}_{2^n}^{n \times n}$ is defined by applying a linear permutation $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ to all elements of H, then the quadratic functions defined by H and H' are EA-equivalent. As the mapping $x \mapsto x^2$ is a linear permutation on account of $\gcd(2, 2^n - 1) = 1$, the proposition is an immediate consequence of this theorem.

Proposition 1. *Suppose $F_1 \in \mathbb{F}_{2^n}[x]$ is a homogeneous quadratic APN function with coefficients in $\mathbb{F}_2$, and H is its corresponding QAM. Let H' be the matrix defined by $H'[i, j] = H[i, j]^2$ for $0 \leq i, j < n$. Then H' is also a QAM, and its corresponding function $F_2 \in \mathbb{F}_2[x]$ is EA-equivalent to F_1.*

The results from Theorems 1, 2 and Proposition 1 are combined into an efficient procedure for searching for quadratic APN functions over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_{2^n}$ in Algorithm 1.

Tables 1, 2, 3, 4 list representatives from all CCZ-equivalence classes found by our method. Note that the search is complete, i.e. the CCZ-equivalence classes containing these representatives cover all possible homogeneous quadratic APN functions with coefficients in $\mathbb{F}_2$ over $\mathbb{F}_{2^n}$ with $4 \leq n \leq 9$.

In dimensions $n \leq 6$, we only find power functions as expected. In dimension $n = 7$, besides three power functions, we find 12 polynomials, among which are two binomials, six quadrinomials, three pentanomials, and three hexanomials. In dimension $n = 8$, we find two power functions and 5 polynomials, which consist of two trinomials, two pentanomials, and one hexanomial. In dimension $n = 9$, we find three power functions, along with 5 polynomials: two of them

have 7 terms, one has 8 terms, and two have 9 terms. All the representatives given in the tables are in shortest possible presentation.

In the case of dimension $n \leq 8$, all of the representatives that we have discovered are identical or equivalent to switching class representatives from [22]. Despite this, in dimension $n = 8$, we discover very "short" and previously undocumented representatives (namely, trinomials) for two of the switching classes from [22]: $x^3 + x^6 + x^{72}$ is CCZ-equivalent to $x^3 + \mathrm{Tr}(x^9)$, and $x^3 + x^6 + x^{144}$ is CCZ-equivalent to $x^9 + \mathrm{Tr}(x^3)$. Both of these trinomials consist of monomials from the cyclotomic cosets of x^3 and x^9, and despite their nearly identical structure, they belong to distinct CCZ-equivalence classes. Note that the $x^3 + \mathrm{Tr}(x^9)$ belongs to the infinite family of APN functions from [13], while the second has not be generalized into any infinite family so far.

Furthermore, in dimension $n = 9$, we discover two representatives, viz.

$$s_1(x) = x^{136} + x^{132} + x^{96} + x^{80} + x^{36} + x^{34} + x^{18} + x^{17} + x^{12}$$

and

$$s_2(x) = x^{288} + x^{272} + x^{264} + x^{160} + x^{144} + x^{130} + x^{48} + x^{34}$$

which are CCZ-inequivalent to any currently known APN function over $\mathbb{F}_{2^9}$.

4 Conclusion

We have described a procedure for searching for quadratic APN functions with coefficients in $\mathbb{F}_2$ over $\mathbb{F}_{2^n}$ by constructing matrices of a particular type, and have used this procedure to classify all such functions over the finite fields $\mathbb{F}_{2^n}$ with $n \leq 9$. We have discovered two previously unknown APN functions over $\mathbb{F}_{2^9}$, and a representation of two of the switching class representatives over $\mathbb{F}_{2^8}$ in the form of trinomials, which is simpler than their currently known representations. In the case of $6 \leq n \leq 8$, we have experimentally verified that there are no quadratic APN functions with coefficients in $\mathbb{F}_2$ other than the previously known ones.

Suppose $n = 2m - 1 (m > 2)$;
$NF = \{x : x \in \mathbb{F}_{2^n}^{\star}\}$;
For any index i, j,

$$i + j = \begin{cases} 1, & \text{if } i + j \bmod n = 0, \\ i + j \bmod n, & \text{others.} \end{cases}$$

GetNoneSquare(n): Return a set without $a = b^{2^k}$ for any $a, b \in NF$ and $1 \leq k \leq n - 1$. Exclude some equivalent situation based on Proposition 1.

Input: A zero matrix $H \in \mathbb{F}_{2^n}^{n \times n}$; An index $j (2 \leq j \leq m)$.

Output: Quadratic APN polynomials in $\mathbb{F}_2[x]$;

```
procedure TranFirRow(j, H); W = GetElemC(j, H);
if j = m then
    for each w ∈ W do
        H[1, j] = w; H[j, 1] = w;
        for each t ∈ [1..n − 1] do
            H[1 + t, j + t] = H[t, j + t − 1]^2;
            H[j + t, t + 1] = H[1 + t, j + t];
        end
        if H is QAM then
            Output the corresponding function of H;
        end
    end
else
    for each w ∈ W do
        H[1, j] = w; H[j, 1] = w;
        for each t ∈ [1..n − 1] do
            H[1 + t, j + t] = H[t, j + t − 1]^2;
            H[j + t, t + 1] = H[1 + t, j + t];
        end
        TranFirRow(j + 1, H);
    end
end
end procedure
function GetElemC(j, H);
resu = NF;
if j = 2 then
    resu=GetNoneSquare(n);
else
    S=Span({H[1, i], H[1, n + 2 − i] : i ∈ [2..j − 1]});
    if #S < 2^(2j−4) then
        return { };
    end
    resu=resu diff S;
    for each r ∈ resu do
        H[1, j] = r;
        A=Submatrix(H, 1, 1, j − 1, j);
        if A is not proper then
            resu=resu diff {r};
        end
    end
end
return resu;
end function
```

Table 1: n=4,5,6

n	Functions
4	x^3
5	x^3, x^5
6	x^3

Table 2: n=7

x^3
x^9
x^5
$x^3 + x^9 + x^{18} + x^{66}$
$x^5 + x^{18} + x^{34}$
$x^3 + x^6 + x^{20}$
$x^3 + x^{17} + x^{20} + x^{34} + x^{66}$
$x^3 + x^{17} + x^{33} + x^{34}$
$x^3 + x^5 + x^{10} + x^{33} + x^{34}$
$x^3 + x^9 + x^{18} + x^{66}$
$x^3 + x^{12} + x^{17} + x^{33}$
$x^3 + x^{20} + x^{34} + x^{66}$
$x^3 + x^{12} + x^{40} + x^{72}$
$x^3 + x^6 + x^{34} + x^{40} + x^{72}$
$x^3 + x^5 + x^6 + x^{12} + x^{33} + x^{34}$

Table 3: n=8

x^3
x^9
$x^3 + x^6 + x^{72}$
$x^3 + x^6 + x^{144}$
$x^3 + x^6 + x^{68} + x^{80} + x^{132} + x^{160}$
$x^3 + x^5 + x^{18} + x^{40} + x^{66}$
$x^3 + x^{12} + x^{40} + x^{66} + x^{130}$

Table 4: n=9

x^3
x^5
x^{17}
$x^{136} + x^{132} + x^{96} + x^{80} + x^{36} + x^{34} + x^{18} + x^{17} + x^{12}$
$x^{257} + x^{144} + x^{130} + x^{72} + x^{65} + x^{18} + x^9$
$x^{144} + x^{130} + x^{72} + x^{65} + x^{18} + x^9 + x^3$
$x^{264} + x^{160} + x^{144} + x^{132} + x^{80} + x^{72} + x^{66} + x^{40} + x^{17}$
$x^{288} + x^{272} + x^{264} + x^{160} + x^{144} + x^{130} + x^{48} + x^{34}$

References

[1] Biham E., Shamir A.: Differential cryptanalysis of DES-like cryptosystems., Journal of Cryptology, vol. 4, no. 1, pp. 3-72, 1991.

[2] Bracken C, Byrne E, Markin N, McGuire G.: A few more quadratic APN functions, Cryptogr. Commun., vol. 3, no. 3, pp. 43-53, 2011.

[3] Brinkmann M., Leander G.: On the classification of APN functions up to dimension five, Designs, Codes and Cryptography,vol. 49, no.1-3, pp. 273 - 288, 2008.

[4] Browning K., Dillon J F., McQuistan M.: APN polynomials and related codes, Special volume of Journal of Combinatorics, Information and System Sciences, honoring the 75-th birthday of Prof. D.K.Ray-Chaudhuri, vol. 34, no. 1-4, pp. 135-159, 2009.

[5] Browning K, Dillon J. F., McQuistan M., Wolfe A. J.: An APN permutation in dimension six, Contemporary Mathematics, vol. 58, pp. 33-42, 2010.

[6] Budaghyan L.: Construction and Analysis of Cryptographic Functions. Springer Verlag, 2014.

[7] Budaghyan L., Carlet C., Pott A.: New classes of almost bent and almost perfect nonlinear polynomials, IEEE Trans. Inf. Theory, vol. 52, no. 3, pp. 1141-1152, 2006.

[8] Budaghyan L., Carlet C.: Classes of quadratic APN trinomials and hexanomials and related structures, IEEE Trans. Inf. Theory, vol. 54, no. 5, pp. 2354-2357, 2008.

[9] Budaghyan L., Calderini C., Carlet C., Coulter R., Villa I.: Constructing APN functions through isotopic shifts, https://eprint.iacr.org/2018/769.

[10] Budaghyan L., Carlet C., Felke P., Leander G.: An infinite class of quadratic APN functions which are not equivalent to power mappings, IEEE International Symposium on Information Theory, pp. 2637-2641, 2006.

[11] Budaghyan L., Helleseth T., Kaleyski N.: A new family of APN quadrinomials, Cryptology ePrint Archive, Report 2019/994, 2019.

[12] Budaghyan L., Carlet C., Leander G.: Two classes of quadratic APN binomials inequivalent to power functions, IEEE Transactions on Information Theory, vol. 54, no. 9, pp. 4218-4229, 2008.

[13] Budaghyan L., Carlet C., G. Leander, Constructing new APN functions from known ones, Finite Fields and Their Appl., vol. 15, no. 2, pp. 150-159, 2009.

[14] Budaghyan L., Carlet C., Leander G.: On a construction of quadratic APN functions, 2009 IEEE Information Theory Workshop, 2009.

[15] Budaghyan L, Helleseth T, Li N, Sun B. Some results on the known classes of quadratic APN functions. InInternational Conference on Codes, Cryptology, and Information Security 2017 Apr 10 (pp. 3-16). Springer, Cham.

[16] Budaghyan L., Calderini M., Villa I.: On equivalence between known families of quadratic APN functions, https://eprint.iacr.org/2019/793.

[17] Calderini M. On the EA-classes of known APN functions in small dimensions, https://eprint.iacr.org/2019/369.

[18] Carlet C.: Vectorial Boolean functions for cryptography. Boolean models and methods in mathematics, computer science, and engineering, Encyclopedia of Mathematics and its Applications, vol. 134, pp. 398-469, 2010.

[19] Carlet C., Charpin P., Zinoviev V.: Codes, bent functions and permutations suitable for DES-like cryptosystems, Designs, Codes and Cryptography, 15(2):125-156, 1998.

[20] Chabaud F, Vaudenay S. Links between differential and linear cryptanalysis. InWorkshop on the Theory and Application of of Cryptographic Techniques 1994 May 9 (pp. 356-365). Springer, Berlin, Heidelberg.

[21] Edel Y.: Quadratic APN functions as subspaces of alternating bilinear forms. Proceedings of the Contact Forum Coding Theory and Cryptography III, Belgium 2011 (Vol. 2009, pp. 11-24).

[22] Yves Edel, Alexander Pott. A new almost perfect nonlinear function which is not quadratic. Advances in Mathematics of Communications, 2009, 3 (1) : 59-81

[23] Langevin P.: Classification of APN cubics in dimension 6 over GF(2). http://langevin.univ-tln.fr/project/apn-6/apn-6.html.

[24] Matsui, M.: Linear cryptanalysis method for DES cipher. Workshop on the Theory and Application of Cryptographic Techniques, Springer, Berlin, Heidelberg, 1993.

[25] Nyberg, K.: Differentially uniform mappings for cryptography. Workshop on the Theory and Application of of Cryptographic Techniques, Springer, Berlin, Heidelberg, 1993.

[26] Taniguchi H.: On some quadratic APN functions, Designs, Codes and Cryptography, vol. 87, no. 9, pp 1973–1983, 2019.

[27] Yu Y., Wang M., Li Y.: A matrix approach for constructing quadratic APN functions.Designs, Codes and Cryptography, vol. 73, no. 2, pp. 587-600, 2014.

[28] Zhou Y., Pott A.: A new family of semifields with 2 parameters. Advances in Mathematics, vol. 234, pp. 43-60, 2013.