Further investigations on the QAM method for Finding APN Functions

Nadiia Ichanska, Nikolay S. Kaleyski

University of Bergen

BFA 2024

September 13, 2024

Vectorial Boolean Functions and APN functions

$\mathbb{F}_{2^n}$ - finite field with 2^n elements, $n \in \mathbb{N}$.

- A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called **(n,n)**-function or **Vectorial Boolean Function**.
- $F(x) = \sum_{i=0}^{2^n-1} a_i \cdot x^i,\ a_i \in \mathbb{F}_{2^n}$ - its **univariate representation.**
- $D_aF(x) = F(a+x) + F(x)$ - its **derivative** in the direction $a \in \mathbb{F}_{2^n} \backslash \{0\}$.
- $\Delta_aF(x) = F(a+x) + F(x) + F(a) + F(0)$ - **symmetric derivative** in the direction $a \in \mathbb{F}_{2^n} \backslash \{0\}$ of F.

Vectorial Boolean Functions and APN functions

$\mathbb{F}_{2^n}$ - finite field with 2^n elements, $n \in \mathbb{N}$.

- A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called **(n,n)**-function or **Vectorial Boolean Function**.
- $F(x) = \sum_{i=0}^{2^n-1} a_i \cdot x^i, \; a_i \in \mathbb{F}_{2^n}$ - its **univariate representation.**
- $\Delta F(a, x) = F(a + x) + F(x) + F(a) + F(0)$ - **symmetric derivative** in the direction $a \in \mathbb{F}_{2^n} \setminus \{0\}$ of F.
- $\delta_F = \max\limits_{a,b \in \mathbb{F}_{2^n}, a \neq 0} |\{x \in \mathbb{F}_{2^n} : \Delta F(a, x) = b\}|$ - its **differential unifomity**.
- F is **almost perfect nonlinear(APN)** if $\delta_F = 2$.

- The **algebraic degree** of a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is $\deg(F) = \max_{\substack{0 \leq i \leq 2^n - 1 \\ a_i \neq 0}} w_2(i)$, where $w_2(i)$ is the 2-weight of the exponent i.
- F is a **linear** function if $F(x) = \sum_{0 \leq i < n} a_i x^{2^i}, \ a_i \in \mathbb{F}_{2^n}$.
- F is **affine** if it is a sum of a linear function and a constant.
- F is **quadratic** if $\deg(F) = 2$.
- We will consider homogeneous quadratic (n, n)-function F

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

Equivalence

The functions F and F' from $\mathbb{F}_{2^n}$ to itself are called

- affine equivalent (or linear equivalent) if $F' = A_1 \circ F \circ A_2$ for affine (linear) permutations A_1, A_2 from $\mathbb{F}_{2^n}$ to itself.
- EA-equivalent if F' and $F + A$ are affine equivalent for an affine mapping A.
- Carlet-Charpin-Zinoviev (CCZ-equivalent).

For quadratic APN (n, n) - functions, F and F' are CCZ-equivalent if and only if they are EA-equivalent [4].

QAM of the quadratic function over $\mathbb{F}_{2^n}$

- Let $F(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j}$ over $\mathbb{F}_{2^n}$.
- Set a normal basis $\mathcal{B} = \{b, b^2, \ldots, b^{2^{n-1}}\}$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.
- The **rank** of the vector $v \in \mathbb{F}_{2^n}^n$ is the dimension of the $\mathbb{F}_2$-subspace spanned by its elements.
- The **derivative matrix** [3], [5] $M_F \in \mathbb{F}_{2^n}^{n \times n}$ of function F is

$$M_F(\mathcal{B}) = \begin{bmatrix} \Delta F(b,b) & \Delta F(b,b^2) & \ldots & \Delta F\left(b, b^{2^{n-1}}\right) \\ \Delta F(b^2,b) & \Delta F(b^2,b^2) & \ldots & \Delta F\left(b^2, b^{2^{n-1}}\right) \\ \vdots & \vdots & \ddots & \vdots \\ \Delta F\left(b^{2^{n-1}}, b\right) & \Delta F\left(b^{2^{n-1}}, b^2\right) & \ldots & \Delta F\left(b^{2^{n-1}}, b^{2^{n-1}}\right) \end{bmatrix}.$$

QAM of the quadratic function over $\mathbb{F}_{2^n}$

The **derivative matrix** $M_F \in \mathbb{F}_{2^n}^{n \times n}$ of function $F(x)$

$$M_F = \begin{bmatrix} \Delta F(b,b) & \Delta F(b,b^2) & \dots & \Delta F\left(b, b^{2^{n-1}}\right) \\ \Delta F(b,b^2) & \Delta F(b^2,b^2) & \dots & \Delta F\left(b^2, b^{2^{n-1}}\right) \\ \vdots & \vdots & \ddots & \vdots \\ \Delta F\left(b, b^{2^{n-1}}\right) & \Delta F\left(b^2, b^{2^{n-1}}\right) & \dots & \Delta F\left(b^{2^{n-1}}, b^{2^{n-1}}\right) \end{bmatrix} \tag{1}$$

is called a **Quadratic APN Matrix (QAM)** [5] if:

1. M_F is symmetric and the elements in its main diagonal are all zeros;
2. Every nonzero linear combination of the n rows (or columns, since M_F is symmetric) of M_F has rank $n-1$.

Following Corollary 5 from [3], we get that the function

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

is APN if and only if its derivative matrix M_F is QAM.

Structure of the derivative matrix (1)

- Let $F(x) = \sum_{0 \leq i < j \leq n-1} a_{i,j} x^{2^i + 2^j}$ with coefficients $a_{i,j} \in \mathbb{F}_{2^m}$,
- $(F(x))^{2^m} = F\left(x^{2^m}\right)$, $(\Delta F(a,x))^{2^m} = \Delta F\left(a^{2^m}, x^{2^m}\right)$;
-
$$M_{i+m,j+m} = (M_{i,j})^{2^m}$$

$$\begin{bmatrix} \Delta F(b,b) & \Delta F(b,b^2) & \Delta F(b,b^{2^2}) & \dots & \Delta F\left(b, b^{2^{n-1}}\right) \\ \Delta F(b^2,b) & \Delta F(b^2,b^2) & \ddots & \dots & \Delta F\left(b^2, b^{2^{n-1}}\right) \\ \ddots & \ddots & \ddots & \ddots & \Delta F(b^{2^2}, b^{2^{n-1}}) \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \Delta F\left(b, b^{2^{n-1}}\right) & \Delta F\left(b^2, b^{2^{n-1}}\right) & \dots & \Delta F\left(b^{2^{n-2}}, b^{2^{n-1}}\right) & \Delta F\left(b^{2^{n-1}}, b^{2^{n-1}}\right) \end{bmatrix}$$

Structure of the derivative matrix (1)

- Let $F(x) = \sum_{0 \leq i < j \leq n-1} a_{i,j} x^{2^i + 2^j}$ with coefficients $a_{i,j} \in \mathbb{F}_{2^m}$
- $(F(x))^{2^m} = F\left(x^{2^m}\right), \quad (\Delta F(a,x))^{2^m} = \Delta F\left(a^{2^m}, x^{2^m}\right)$
- $$M_{i+m,j+m} = (M_{i,j})^{2^m}$$

$$\begin{bmatrix} 0 & \Delta F(b,b^2) & \Delta F(b,b^{2^2}) & \dots & \dots & \Delta F\left(b,b^{2^n}\right) \\ \Delta F(b,b^2) & 0 & \ddots & \dots & \dots & \Delta F\left(b^2,b^{2^n}\right) \\ \Delta F(b,b^{2^2}) & \ddots & \ddots & (\Delta F(b,b^2))^{2^m} & (\Delta F(b,b^{2^2}))^{2^m} & \vdots \\ \vdots & \ddots & (\Delta F(b,b^2))^{2^m} & 0 & \dots & \vdots \\ \vdots & \ddots & (\Delta F(b,b^{2^2}))^{2^m} & \ddots & \dots & \vdots \\ \Delta F\left(b,b^{2^n}\right) & \Delta F\left(b^2,b^{2^n}\right) & \dots & \dots & \dots & 0 \end{bmatrix}$$

Structure of the search

$$
M_F = \begin{pmatrix}
0 & \Omega_1 & \Omega_2 & \Omega_3 & \dots & \dots & \dots & \dots & \dots \\
\Omega_1 & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \dots & \vdots \\
\Omega_2 & \ddots & 0 & \Omega_1^{2^m} & \Omega_2^{2^m} & \Omega_3^{2^m} & \ddots & \dots & \vdots \\
\Omega_3 & \ddots & \Omega_1^{2^m} & 0 & \ddots & \ddots & \ddots & \ddots & \vdots \\
\ddots & \ddots & \Omega_2^{2^m} & \ddots & 0 & \Omega_1^{2^{2m}} & \Omega_1^{2^{2m}} & \Omega_3^{2^{2m}} & \dots \\
\vdots & \ddots & \ddots & \ddots & \Omega_1^{2^{2m}} & \ddots & \ddots & \ddots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots
\end{pmatrix}, \tag{3}
$$

where $\Omega_1, \Omega_2, \dots, \Omega_l$ - **variables**.

A variable Ω_i is located on the i-th **level**.

Orbit restrictions

Theorem 3 [5]

For any linear permutation l on $\mathbb{F}_{2^n}$ and $M \in \mathbb{F}_{2^n}^{n \times n}$ s.t. $M = M_F$ then any $M' = M_{F'}$ produced by

$$M'_{i,j} = l(M_{i,j}) \text{ for all } 1 \leq i, j \leq n \tag{4}$$

will be $F' = l \circ F$ linearly equivalent to F.

Let $\mathcal{L}$ be a set of all linear (n, n)-permutations on $\mathbb{F}_{2^n}$ with subfield $\mathbb{F}_{2^m}$ coefficients. Then the **orbit** of $a \in \mathbb{F}_{2^n}$

$$Orb(a, \mathcal{L}) = \{l(a) : l \in \mathcal{L}\}. \tag{5}$$

Orbit Restrictions

$$\mathbb{F}_{2^n} = Orb(a_1, \mathcal{L}) \cup \cdots \cup Orb(a_k, \mathcal{L}), \text{ for some } a_i \in \mathbb{F}_{2^n}, \ 1 \leq i \leq k.$$

$$M_{F'} = \begin{pmatrix} 0 & L(\Omega_1) & L(\Omega_2) & \dots & \dots & \dots \\ L(\Omega_1) & 0 & \ddots & \ddots & \dots & \dots \\ L(\Omega_2) & \dots & 0 & L(\Omega_1^{2^m}) & L(\Omega_2^{2^m}) & \dots \\ \vdots & \vdots & L(\Omega_1^{2^m}) & 0 & \dots & \dots \\ \vdots & \vdots & L(\Omega_2^{2^m}) & \dots & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix},$$

where $L(\Omega_i^{2^{m*j}}) = (L(\Omega_i))^{2^{m*j}}$, $j \in \{1, \dots, n/m - 1\}$ for any variable Ω_i, $1 \leq i \leq l$.

Orbit partition level by level

$\mathbb{F}_{2^n} = Orb(A, \mathcal{L}) \cup \ldots, \; A \in \mathbb{F}_{2^n}.$

$$M_F = \begin{pmatrix} 0 & A & \Omega_2 & \ldots & \ldots & \ldots \\ A & 0 & \ddots & \ddots & \ldots & \ldots \\ \Omega_2 & \ldots & 0 & A^{2^m} & \Omega_2^{2^m} & \ldots \\ \vdots & \vdots & A^{2^m} & 0 & \ldots & \ldots \\ \vdots & \vdots & \Omega_2^{2^m} & \ldots & 0 & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

$$Orb_A(\Omega_2, \mathcal{L}) = \{ l(\Omega_2) : l \in \mathcal{L} \mid l(A) = A \}.$$

$$S = \{\Omega_1, \ldots, \Omega_{k-1}\}$$

$$Orb_S(\Omega_k, \mathcal{L}) = \{ l(\Omega_k) : l \in \mathcal{L} \mid \forall X \in S : \; l(X) = X \}.$$

Submatrix method

- Let $M \in \mathbb{F}_{2^n}^{n \times n}$ be a derivative matrix.
- M is QAM if and only if every submatrix $S \in \mathbb{F}_{2^n}^{p \times q}$, $1 \leq p, q \leq n$ of M is **proper**.
- S **proper** if every nonzero linear combinations of the p rows has rank at least $q - 1$.

Submatrix method

- Let $M \in \mathbb{F}_{2^n}^{n \times n}$ be a derivative matrix.
- M is QAM if and only if every submatrix $S \in \mathbb{F}_{2^n}^{p \times q}$, $1 \leq p, q \leq n$ of M is **proper**.
- $$\begin{pmatrix} 0 & A & B & \Omega_3 & \dots & \dots \\ A & 0 & \ddots & \ddots & \dots & \dots \\ B & \dots & 0 & A^{2^m} & B^{2^m} & \dots \\ \Omega_3 & \vdots & A^{2^m} & \ddots & \dots & \dots \\ \vdots & \vdots & B^{2^m} & \dots & \dots & 0 \end{pmatrix}.$$
- By considering $F' = F \circ L$, where $L = a_j x^{2^i}$, $a_j \in \mathbb{F}_{2^m}$, we can eliminate the number of submatrices for this test.

$(n, m) = (10, 1)$

- $F(x)$ over $\mathbb{F}_{2^{10}}$ with coefficients in $\mathbb{F}_2$,
- $|\mathcal{L}| = 1024$ linear permutations with coefficients in $\mathbb{F}_2$,
- The number of variables = levels in this dimension is 5.

First level representatives $A \in \mathcal{A}$							
1	a	a^5	a^{15}	a^{33}	a^{57}	a^{99}	a^{341}
Number of orbits $\mathcal{B}_A$ that passed the submatrix test							
0	746	1012	753	71	112	78	8
Number of parallel processes that were done							
-	32	48	32	8	16	8	16
Time taken							
-	2,5 month	3 month	2,6 month	4 days	10 days	12 days	12 days

Found 577 APN functions fell into three CCZ-equivalent classes corresponding to x^3, x^9 and $x^3 + a^{-1}\mathrm{Tr}_n(a^3x^9)$ [1].

$(n, m) = (10, 2)$

- $F(x)$ over $\mathbb{F}_{2^{10}}$ with coefficients in $\mathbb{F}_{2^2}$,
- $4^{10} = 1048576$ linear function with coefficients in the subfield were constructed, where 367200 permutations,
- The number of variables = levels in this dimension is 9.

First level representatives $A \in \mathcal{A}$		
1	a	a^5
Number of orbits $\mathcal{B}_A$ that passed the submatrix test		
3	28	46
Number of orbits $\mathcal{C}_{B,a}$ that passed the submatrix test		
80		
Average number of orbits $\mathcal{D}_{C,B,a}$ that passed the submatrix test		
64		
Number of parallel processes that were done		
32		
3 months and not finished		

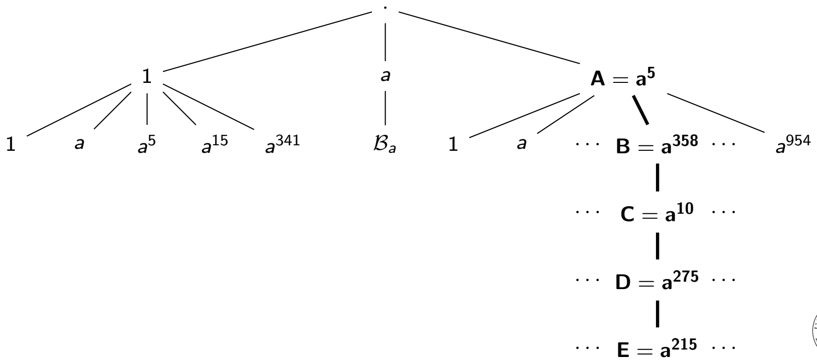
$(n, m) = (10, 2)$

- $F(x)$ over $\mathbb{F}_{2^{10}}$ with coefficients in $\mathbb{F}_{2^2}$,
- $4^{10} = 1048576$ linear function with coefficients in the subfield were constructed, where 367200 permutations,
- The number of variables = levels in this dimension is 9.

First level representatives $A \in \mathcal{A}$		
1	a	a^5
Number of orbits $\mathcal{B}_A$ that passed the submatrix test		
3	28	46
Number of orbits $\mathcal{C}_{B,a}$ that passed the submatrix test		
80		
Average number of orbits $\mathcal{D}_{C,B,a}$ that passed the submatrix test		
64		
Number of parallel processes that were done		
32		
3 months and not finished		

$(n, m) = (10, 2)$ with the first 5 levels fixed

- The known APN [2] $F = x^{288} + a^{682}x^{96} + a^{341}x^{9} + x^{3}$ (3),
- The normal basis with the base a^{486},
- The search took 10 days and found only (3).



$(n, m) = (10, 2)$ with first 5 levels fixed

Problem

First N variables of the derivative matrix M characterize ≤ 1 possible APN function F over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_{2^m}$.

Partial backward search for $F = x^{288} + a^{682}x^{96} + a^{341}x^9 + x^3$

$A = a^5, B = a^{358}, C = a^{10}, D = a^{275}$; $\forall E \in \mathcal{E}^{Sub}_{A,B,C,D} \setminus \{a^{215}\}$,

$|\mathcal{E}^{Sub}_{A,B,C,D}| = 900.$

$E = a^{884}$ - 15,5 days in 32 cores;
$E = a^{189}$ - 15 days in 32 cores;
$E = a^{796}$ - 14 days in 32 cores;

Can we partition into orbits without the set of linear permutations?

- For cases $(9,3)$ and $(8,4)$ we get $(2^3)^9$ and $(2^4)^8$ linear functions;
- Case $(10,2)$ gets an "Out of Memory error" for low-memory servers (i.e. 64 GB RAM);
- More permutations - better partition.

Algorithm for partitioning without pre-generated $\mathcal{L}$

Lemma 1

Let $a \in \mathbb{F}_{2^n}$. We categorize a into the following cases:

1. $Cat_1 = \{a : a \in \mathbb{F}_{2^n} \mid a + a^{2^m} = 0\}$,
2. $Cat_2 = \{a : a \in \mathbb{F}_{2^n} \mid a + a^{2^m} + a^{2^{2m}} + \cdots + a^{2^{n-m}} = 0\}$,
3. $Cat_3 = \{a : a \in \mathbb{F}_{2^n} \mid a + a^{2^m} + a^{2^{2m}} = 0\}$,

   ...

4. $Cat_{Ind} = \{a : a \in \mathbb{F}_{2^n} \mid a \notin Cat_i \text{ for any } i\}$,

Theorem 1

Let $a, b \in Cat_{Ind}$. If there exists $l(x) = \sum_{i=0}^{n-1} c_i x^{2^i},\ c_i \in \mathbb{F}_{2^m}$ s.t. $l(a) = b,\ l(a^{2^m}) = b^{2^m}, \ldots,\ l(a^{2^{n-m}}) = b^{2^{n-m}}$. Then there exists a linear permutation $L \in \mathcal{L}$ s.t. $L(a) = b$.

$(n, m) = (9, 3)$

- $F(x)$ over $\mathbb{F}_{2^9}$ with coefficients in $\mathbb{F}_{2^3}$.
- The number of variables = levels in this dimension is 12.
- Let $a \in \mathbb{F}_{2^9}$. Then a can be categorized into the following cases:
  1. $Cat_1 = \{a : a \in \mathbb{F}_{2^9} \mid a + a^{2^3} = 0\}$,
  2. $Cat_2 = \{a : a \in \mathbb{F}_{2^9} \mid a + a^{2^3} + a^{2^6} = 0\}$,
  3. $Cat_{Ind} = \{a : a \in \mathbb{F}_{2^9} \mid a \notin Cat_1,\ a \notin Cat_2\}$,

Corollary 1

Let $a, b \in Cat_{Ind}$. If there exist $l(x) = \sum_{i=0}^{9} c_i x^{2^i},\ c_i \in \mathbb{F}_{2^3}$ s.t. $l(a) = b,\ l(a^{2^3}) = b^{2^3},\ l(a^{2^6}) = b^{2^6}$. Then there exists a linear permutation $L \in \mathcal{L}$ s.t. $L(a) = b$.

$(n, m) = (8, 4)$

- $F(x)$ over $\mathbb{F}_{2^8}$ with coefficients in $\mathbb{F}_{2^4}$.
- The number of variables = levels in this dimension is 16, with 4 them in the subfield.
- Let $a \in \mathbb{F}_{2^8}$. Then a can be categorized into the following cases:
    1. $Cat_1 = \{a : a \in \mathbb{F}_{2^8} \mid a + a^{2^4} = 0\}$,
    2. $Cat_{Ind} = \{a : a \in \mathbb{F}_{2^8} \mid \; a \notin Cat_1\}$,

Corollary 2

Let $a, b \in Cat_{Ind}$. If there exist $l(x) = \sum_{i=0}^{8} c_i x^{2^i}, \; c_i \in \mathbb{F}_{2^4}$ s.t. $l(a) = b, \; l(a^{2^4}) = b^{2^4}$. Then there exists a linear permutation $L \in \mathcal{L}$ s.t. $L(a) = b$.

Partition on the second level

We fix $A \mapsto A$ on the first level.

Theorem 2

1. For $A \in Cat_{Ind}$, we get $\forall a, b \in \mathbb{F}_{2^n}$: $a \sim b$, if there exist $l(x) = \sum_{i=0}^{8} c_i x^{2^i}$, $c_i \in \mathbb{F}_{2^4}$ s.t. $l(a) = b,\ l(a^{2^4}) = b^{2^4},\ l(A) = A,\ l(A^{2^4}) = A^{2^4}$.
2. For $A \in Cat_1$, we get $\forall a, b \in \mathbb{F}_{2^n}$: $a \sim b$, if there exist $l(x) = \sum_{i=0}^{8} c_i x^{2^i}$, $c_i \in \mathbb{F}_{2^4}$ s.t. $l(a) = b,\ l(a^{2^4}) = b^{2^4},\ l(b) = a,\ l(b^{2^4}) = a^{2^4},\ l(A) = A$.

Partitioning until k-th level

Theorem 3

For $\Omega_1, \Omega_2, \ldots, \Omega_k \in Cat_{Ind}$. After we fixed k variables, in order to partition $k+1$-level:

1. Choose $\Omega_{k+1} \in Cat_{Ind}$ s.t. $\{\Omega_1, \ldots, \Omega_{k+1}\}$ - linearly independent set of vectors;
2. Then $\forall a, b \in \mathbb{F}_{2^n}$: $a \sim b$, if there exist $l(x) = \sum_{i=0}^{8} c_i x^{2^i}$, $c_i \in \mathbb{F}_{2^4}$ s.t. $l(a) = b$, $l(a^{2^4}) = b^{2^4}, l(b) = a$, $l(b^{2^4}) = a^{2^4}$, $\forall i \in \{1, \ldots, k+1\} : l(\Omega_i) = \Omega_i$, $l(\Omega_i^{2^4}) = \Omega_i^{2^4}$.

We could efficiently partition A, B, C, D, E, F, G, H in our search; with brute-forcing last 8 levels. Partial search with all restrictions for this case takes 6 days to finish into 64 parallel processes.

Conclusions

- For $F(x)$ over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_{2^m}$ we run searches (n, m) for $(10, 2), (10, 1), (9, 3), (8, 4)$;
- We provide a classification for all quadratic APN functions with coefficients in $\mathbb{F}_2$ over $\mathbb{F}_{2^{10}}$;
- A method for applying the orbit partitioning algorithm for cases where it did not work before was proposed.

Future work

1. How many variables of the derivative matrix define the APN function?
2. How to identify the branches that contain QAM?
3. Optimize the method, implementation, and classification for other choices of (n, m).

References

Lilya Budaghyan, Claude Carlet, and Gregor Leander.
Constructing new APN functions from known ones, 2009.

Lilya Budaghyan, Tor Helleseth, and Nikolay Kaleyski.
A new family of APN quadrinomials.
IEEE Transactions on Information Theory, 66(11):7081–7087, 2020.

Diana Davidova and Nikolay Kaleyski.
Classification of all DO planar polynomials with prime field coefficients over $GF(3^n)$ for n up to 7.
Cryptology ePrint Archive, Paper 2022/1059, 2022.

Satoshi Yoshiara.
Equivalences of quadratic APN functions.
Journal of Algebraic Combinatorics, 35(3):461–475, 2012.

Yuyin Yu, Mingsheng Wang, and Yongqiang Li.
A matrix approach for constructing quadratic APN functions.
Designs, codes and cryptography, 73(2):587–600, 2014.