EA-equivalence Classes of Known APN Functions in Small Dimensions

Marco Calderini

University of Bergen

Boolean Functions and their Applications
June 16-21, 2019

Notations and definitions

PN and APN functions:

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a Vectorial Boolean function. We define

$$\delta_F(a,b) = |\{x \in \mathbb{F}_2^n : F(x+a) - F(x) = b\}|.$$

The **differential uniformity** of F is

$$\delta(F) = \max_{a \in \mathbb{F}_2^n \setminus \{0\},\, b \in \mathbb{F}_2^m} \delta_F(a,b).$$

If $\delta(F) = 2^{n-m}$ then F is said **Perfect Nonlinear** (PN) or **Bent**.
Best resistance to differential attack.

K. Nyberg: Bent functions exist only when n is even and $m \leq n/2$.

If $m = n$, then $\delta(F) \geq 2$.

If $\delta(F) = 2$, then F is called **almost perfect nonlinear** (APN).

AB functions:

The **nonlinearity** of a vectorial Boolean function F is the minimum Hamming distance between

- all component functions $v \cdot F(x)$, $v \neq 0$ and
- all affine functions $u \cdot x + \varepsilon$, $u \in \mathbb{F}_2^n$ $\varepsilon \in \mathbb{F}_2$.

The nonlinearity can be given in terms of the **Walsh transform** of F

$$\mathscr{W}_F(a,b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x + b \cdot F(x)}.$$

The nonlinearity equals:

$$\mathscr{N}\ell(F) = 2^{n-1} - \frac{1}{2} \max_{\substack{a \in \mathbb{F}_2^n, \\ b \in \mathbb{F}_2^m \setminus \{0\}}} |\mathscr{W}_F(a,b)|.$$

Bounds on nonlinearity

$$\mathcal{N}\ell(F) \leq 2^{n-1} - 2^{n/2-1}.$$

The equality holds iff F is bent (best resistance to linear attack).
If $n = m$ the Sidelnikov-Chabaud-Vaudenay bound states

$$\mathcal{N}\ell(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}.$$

In case of equality (n necessarily odd) F is called **almost bent** (AB).

AB $\Rightarrow$ APN

From now on, we assume that $m = n$. In this case we can identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$ and then we can take $x \cdot y = tr(xy)$.

Table: Known APN power functions x^d over $\mathbb{F}_{2^n}$

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

Table: Known APN power functions x^d over $\mathbb{F}_{2^n}$

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

Gold, Kasami, Welch and Niho functions are AB for n odd

Equivalence relations

Two functions $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are **affine equivalent** iff

$$G = A_2 \circ F \circ A_1(x),$$

with A_1 and A_2 affine permutations.

Equivalence relations

Two functions $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are **affine equivalent** iff

$$G = A_2 \circ F \circ A_1(x),$$

with A_1 and A_2 affine permutations.

$$\cap$$

Two functions $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are **EA-equivalent** iff

$$G = A_2 \circ F \circ A_1(x) + A(x),$$

with A, A_1 and A_2 affine maps and A_1 and A_2 permutations.

Equivalence relations

Two functions $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are **affine equivalent** iff

$$G = A_2 \circ F \circ A_1(x),$$

with A_1 and A_2 affine permutations.

$$\cap$$

Two functions $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are **EA-equivalent** iff

$$G = A_2 \circ F \circ A_1(x) + A(x),$$

with A, A_1 and A_2 affine maps and A_1 and A_2 permutations.

$$\cap$$

Let $\Gamma_f = \{(x, f(x)) \mid x \in \mathbb{F}_{2^n}\}$.
Two functions $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are **CCZ-equivalent** if and only if Γ_F and Γ_G are affine-equivalent, i.e. let $\mathscr{L}$ an affine permutation on $(\mathbb{F}_{2^n})^2$, $\mathscr{L}(\Gamma_F) = \Gamma_G$.

CCZ-equivalence

Let $\mathscr{L}$ be a linear permutation of $(\mathbb{F}_{2^n})^2$ such that $\mathscr{L}(\Gamma_F) = \Gamma_G$.
$\mathscr{L} = (L_1, L_2)$ for some linear $L_1, L_2 : (\mathbb{F}_{2^n})^2 \to \mathbb{F}_{2^n}$. Then

$$\mathscr{L}(x, F(x)) = (F_1(x), F_2(x)),$$

where $F_1(x) = L_1(x, F(x))$ and $F_2(x) = L_2(x, F(x))$.

$$\mathscr{L}(\Gamma_F) = \{(F_1(x), F_2(x)) : x \in \mathbb{F}_{2^n}\}.$$

$\mathscr{L}(\Gamma_F)$ is the graph of G iff the function F_1 is a permutation and $G = F_2 \circ F_1^{-1}$

If we want to construct G which can be obtained from F via CCZ-equivalence:

- Find a permutation $L_1(x, F(x)) = L(x) + R \circ F(x)$ where L, R are linear.
- Then find linear function $L_2(x, y) = L'(x) + R'(y)$ such that $\mathscr{L}$ is a permutation. (Found L_1 then there always exists suitable L_2)

Relation between CCZ- and EA-equivalences

Cases when CCZ-equivalence coincides with EA-equivalence:

- Boolean functions, $m = 1$. (Budaghyan and Carlet)
- Bent functions. (Budaghyan and Carlet)
- Two quadratic APN functions. (Yoshiara)
- A power function F is CCZ-equivalent to a power function F' iff F is EA-equivalent to F' or F'^{-1}. (for APN and $p = 2$ Yoshiara, any p and any power Dempwolff)
- A quadratic APN function is CCZ-equivalent to a power function iff it is EA-equivalent to one of the Gold functions. (Yoshiara)
- If n is even, a plateaued APN function is CCZ-equivalent to a plateaued power function iff it is EA-equivalent to it. (Yoshiara)

Cases when CCZ-equivalence differs from EA-equivalence:

- For functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ with $m \geq 2$.

Equivalences of Boolean functions and codes

Let F be a vectorial Boolean function over $\mathbb{F}_{2^n}$ then we can associate to F the linear code $\mathscr{C}_1(F)$ generated by

$$C_1(F) = \begin{bmatrix} 1 \\ x \\ F(x) \end{bmatrix}_{x \in \mathbb{F}_{2^n}} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 0 & u & \dots & u^{2^n-1} \\ F(0) & F(u) & \dots & F(u^{2^n-1}) \end{bmatrix}$$

Theorem (Browning, Dillon, Kibler, McQuistan)

Let F and G be two vectorial Boolean function over $\mathbb{F}_{2^n}$. Then, F is CCZ-equivalent to G iff $\mathscr{C}_1(F)$ is equivalent to $\mathscr{C}_1(G)$.

Equivalence of Boolean functions and codes

Let $\mathscr{C}_2(F)$ generated by

$$C_2(F) = \begin{bmatrix} 1 & 0 \\ x & 0 \\ F(x) & y \end{bmatrix}_{x \in \mathbb{F}_{2^n}, y \in \mathbb{F}_{2^n}^*}$$

Theorem (Edel, Pott)

Let F and G be two vectorial Boolean function over $\mathbb{F}_{2^n}$. Then, F is EA-equivalent to G iff $\mathscr{C}_2(F)$ is equivalent to $\mathscr{C}_2(G)$.

Equivalence of Boolean functions and codes

Let $\mathscr{C}_3(F)$ generated by

$$C_3(F) = \begin{bmatrix} 1 & 0 & 0 \\ x & 0 & z \\ F(x) & y & 0 \end{bmatrix}_{x \in \mathbb{F}_{2^n}, y,z \in \mathbb{F}_{2^n}^*}$$

Theorem (Edel, Pott)

Let F and G be two vectorial Boolean function over $\mathbb{F}_{2^n}$. If F is not a permutation, then F is affine-equivalent to G iff $\mathscr{C}_3(F)$ is equivalent to $\mathscr{C}_3(G)$.
If F is a permutation, then F is affine-equivalent to G or G^{-1} iff $\mathscr{C}_3(F)$ is equivalent to $\mathscr{C}_3(G)$.

Remark

If F is a permutation, we may not be able to distinguish whether F is equivalent to G or G^{-1}.

Equivalence of Boolean functions and codes

An extra code for the permutation case: Let $\mathscr{C}_4(F)$ generated by

$$C_4(F) = \begin{bmatrix} 1 & 0 & 1 \\ x & 0 & z \\ F(x) & y & 0 \end{bmatrix}_{x,z \in \mathbb{F}_{2^n}, y \in \mathbb{F}_{2^n}^*}$$

Theorem

Let F and G be two permutations over $\mathbb{F}_{2^n}$, with $n \geq 3$. F is affine-equivalent to G iff $\mathscr{C}_4(F)$ is equivalent to $\mathscr{C}_4(G + b)$ for some $b \in \mathbb{F}_{2^n}$.

Classification of APN functions

- $n = 3, 4$ full classification with respect to the affine equivalence of all permutations (Leander, Poschmann).
- $n = 3, 4$ full classification with respect to the CCZ-equivalence and EA-equivalence of all functions over $\mathbb{F}_{2^n}$ (Brinkmann).
- $n \leq 5$ full classification of all APN functions with respect to the CCZ-equivalence and EA-equivalence (Brinkmann, Leander).
- $n = 6$ full classification of cubic APN functions with respect to the CCZ-equivalence (Langevin, Z. Saygi, E. Saygi).
- $n \leq 11$ classification with respect to the CCZ-equivalence of APN functions from all known families of APN functions (Sun).

A procedure for investigating if $CCZ \stackrel{?}{=} EAI$[1]

Let $L_1(x,y) = L(x) + R(y)$. $F_1(x) = L(x) + R(F(x))$ is a permutation iff any of its component is balanced.
In terms of Walsh coefficients

$$\mathscr{W}_{F_1}(0,\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr(\lambda L(x) + \lambda R \circ F(x))} = 0, \quad \text{for all } \lambda \in \mathbb{F}_{2^n}^*.$$

$$\Downarrow$$

$$\mathscr{W}_{F_1}(0,\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr(L^*(\lambda)x + R^*(\lambda)F(x))} = \mathscr{W}_F(L^*(\lambda), R^*(\lambda)).$$

(L^* is the adjoint operator)

[1] Budaghyan, L., Calderini, M., Villa, I., On relations between CCZ- and EA-equivalences. Cryptogr. Commun. (2019)

We want to construct L^* and R^* so that F_1 is a permutation.
Let $\mathscr{ZW}(b) = \{a \mid \mathscr{W}_F(a,b) = 0\}$ for any $b \in \mathbb{F}_{2^n}$ and consider

$$S_F = \{b : \mathscr{ZW}(b) \neq \emptyset\}.$$

Note: if F_1 is a permutation then $Im(R^*) \subseteq S_F$.
For constructing F_1 we need to consider the possible vector subspaces contained in S_F.

Construction of R^*

Let $U \subseteq S_F$ be a vector subspace. Fixed any basis $\{u_1, \dots, u_k\}$ of U, we can suppose that $R^*(e_i) = u_i$ for $i = 1, ..., k$ and $\mathrm{Ker}(R^*) = \mathrm{Span}(e_{k+1}, ..., e_n)$.
(e_i is the canonical vector.)

Fixed any basis $\{u_1, \dots, u_k\}$ of U we can suppose that

$$R^* = \begin{bmatrix} u_1 \\ \vdots \\ u_k \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Construction of L^*

For any $a_1, ..., a_k$ with $a_1 \in \mathscr{Z}\mathscr{W}(u_1), ..., a_k \in \mathscr{Z}\mathscr{W}(u_k)$ we need to check if

(P1) $\sum_{i=1}^{k} \lambda_i a_i \in \mathscr{Z}\mathscr{W}(\sum_{i=1}^{k} \lambda_i u_i)$ with $\lambda_i \in \mathbb{F}_2$ not all zero.

and if there exist $a_{k+1}, ..., a_n$ satisfying

(P2) $a_{k+1}, ..., a_n$ are linear independent;

(P3) for any $a \in Span(a_{k+1}, ..., a_n)$, $a + \sum_{i=1}^{k} \lambda_i a_i \in \mathscr{Z}\mathscr{W}(\sum_{i=1}^{k} \lambda_i u_i)$, for any $\lambda_1, \ldots, \lambda_k \in \mathbb{F}_2$.

Then,

$$L^* = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$$

Functions in the same EA-class

Proposition (Budaghyan, Carlet, Pott)

For a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, if $\mathscr{L} = (L_1, L_2)$ and $\mathscr{L}' = (L_1, L_2')$ are linear permutations such that the function $L_1(x, F(x))$ is a permutation, then the functions defined by the graphs $\mathscr{L}(\Gamma_F)$ and $\mathscr{L}'(\Gamma_F)$ are EA-equivalent.

Thus, fixed L_1, we need to construct just one L_2.

Functions in the same EA-class

Proposition (Budaghyan, Carlet, Pott)

For a function $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$, if $\mathscr{L}=(L_1,L_2)$ and $\mathscr{L}'=(L_1,L_2')$ are linear permutations such that the function $L_1(x,F(x))$ is a permutation, then the functions defined by the graphs $\mathscr{L}(\Gamma_F)$ and $\mathscr{L}'(\Gamma_F)$ are EA-equivalent.

Thus, fixed L_1, we need to construct just one L_2.

Proposition

Let F be a function over $\mathbb{F}_{2^n}$ and let $\mathscr{L}=(L_1,L_2)$ and $\mathscr{L}'=(L_1',L_2')$ be two linear permutations over $(\mathbb{F}_{2^n})^2$ such that $F_1(x)=L_1(x,F(x))$ and $F_1'(x)=L_1'(x,F(x))$ are permutations. If $L_1'(x,y)=L\circ L_1(x,y)$ for some linear permutation L, then the functions defined by the graphs $\mathscr{L}(\Gamma_F)$ and $\mathscr{L}'(\Gamma_F)$ are EA-equivalent.

An upper bound

Corollary

Let F be a function defined over $\mathbb{F}_{2^n}$ with $\mathscr{N}\ell(F) \neq 0$ $(F(0) = 0)$. Let $\mathscr{C}(F)$ be the code generated by

$$\begin{pmatrix} x \\ F(x) \end{pmatrix}_{x \in \mathbb{F}_{2^n}^*}.$$

Let N_{sc} be the number of simplex codes in $\mathscr{C}(F)$. Then

$$\#\textit{EA-classes} \leq N_{sc}.$$

Obtaining the EA-classes

Proposition (Budaghyan, -, Villa)

Let U be a subspace contained in S_F. Then, there exists a permutation of $\mathbb{F}_{2^n}$ $F_1(x) = L(x) + R \circ F(x)$, with L and R linear and $\mathrm{Im}(R^*) = U$, if and only if the procedure applied to the space U is successful.

Proposition

Applying the procedure to all the subspace U contained in S_F, and considering all the L_1's constructed by this procedure, we can obtain at least one representative for each EA-class contained in the CCZ-class of F.

Obtaining the EA-classes

- Use the procedure of Budaghyan, Calderini and Villa for obtaining at least one L_1 for any EA-class.
- If L_1 and L_1' are s.t. the codes generate by $(L_1(x, F(x)))_{x \in \mathbb{F}_{2^n}}$ and $(L_1'(x, F(x)))_{x \in \mathbb{F}_{2^n}}$ are equal, then discard L_1'.
- Construct one L_2 for any L_1 and the related function $F' = F_2 \circ F_1^{-1}$.
- Check the EA-equivalence of all F''s using code equivalence.

The case n=6

Over $\mathbb{F}_{2^6}$ we have

- 14 APN functions (up to CCZ-equivalence) of degree at most 3;
- 13 quadratics APN functions;
- 1 APN function CCZ-inequivalent to quadratic functions
- only one is equivalent to a permutation

EA-classes in dimension 6

Table: CCZ-inequivalent APN functions over $\mathbb{F}_{2^6} = \langle \zeta \rangle$

N.	function	# EA-classes	Degrees
1	x^3	3	{*2,3,4*}
2	$x^3 + \zeta^{11}x^6 + ux^9$	3	{* 2, 3, 4 *}
3	$\zeta x^5 + x^9 + \zeta^4 x^{17} + \zeta x^{18} + \zeta^4 x^{20} + \zeta x^{24} + \zeta^4 x^{34} + \zeta x^{40}$	19	{* 2, 3^^15, 4^^3 *}
4	$\zeta^7 x^3 + x^5 + \zeta^3 x^9 + \zeta^4 x^{10} + x^{17} + \zeta^6 x^{18}$	13	{*2, 3^^9, 4^^3 *}
5	$x^3 + \zeta x^{24} + x^{10}$	13	{*2, 3^^5, 4^^7 *}
6	$x^3 + \zeta^{17}(x^{17} + x^{18} + x^{20} + x^{24})$	91	{*2, 3^^66, 4^^24 *}
7	$x^3 + \zeta^{11}x^5 + \zeta^{13}x^9 + x^{17} + \zeta^{11}x^{33} + x^{48}$	19	{*2, 3^^15, 4^^3 *}
8	$\zeta^{25}x^5 + x^9 + \zeta^{38}x^{12} + \zeta^{25}x^{18} + \zeta^{25}x^{36}$	85	{*2, 3^^66, 4^^18 *}
9	$\zeta^{40}x^5 + \zeta^{10}x^6 + \zeta^{62}x^{20} + \zeta^{35}x^{33} + \zeta^{15}x^{34} + \zeta^{29}x^{48}$	91	{*2, 3^^63, 4^^27 *}
10	$\zeta^{34}x^6 + \zeta^{52}x^9 + \zeta^{48}x^{12} + \zeta^6 x^{20} + \zeta^9 x^{33} + \zeta^{23}x^{34} + \zeta^{25}x^{40}$	91	{*2, 3^^66, 4^^24 *}
11	$x^9 + \zeta^4(x^{10} + x^{18}) + \zeta^9(x^{12} + x^{20} + x^{40})$	86	{*2, 3^^69, 4^^16 *}
12	$\zeta^{52}x^3 + \zeta^{47}x^5 + \zeta x^6 + \zeta^9 x^9 + \zeta^{44}x^{12} + \zeta^{47}x^{33} + \zeta^{10}x^{34} + \zeta^{33}x^{40}$	92	{*2, 3^^69, 4^^22 *}
13	$\zeta(x^6 + x^{10} + x^{24} + x^{33}) + x^9 + \zeta^4 x^{17}$	85	{*2, 3^^66, 4^^18 *}
14	$x^3 + \zeta^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + \zeta^{14}(tr(\zeta^{52}x^3 + \zeta^6 * x^5 + \zeta^{19}x^7 + \zeta^{28}x^1 1 + \zeta^2 x^{13}) +$ $(\zeta^2 x)^9 + (\zeta^2 x)^{18} + (\zeta^2 x)^{36} + x^{21} + x^{42})$	25	{*3^^10, 4^^15 *}

Dillon's APN permutation

Theorem (Browning, Dillon, Kibler, McQuistan)

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be APN, with $F(0) = 0$. F is CCZ equivalent to an APN permutation iff $\mathscr{C}(F)$ is a double simplex code (i.e. $\mathscr{C}(F) = C_1 \oplus C_2$ with C_i a $[2^n - 1, n, 2^{n-1}]$-code).

If F is APN and $\mathscr{C}(F) = C_1 \oplus C_2 = \langle F_1(x) \rangle \oplus \langle F_2(x) \rangle$ is a double simplex code

$$\begin{array}{l} C_1\{ \\ C_2\{ \end{array} \left.\begin{bmatrix} \dots & F_1(x) & \dots \\ \dots & F_2(x) & \dots \end{bmatrix}\right\} \mathscr{C}(F)$$

where $F_i(x) = L_i(x, F(x))$ (L_i linear map from $\mathbb{F}_2^{2n}$ to $\mathbb{F}_2^n$)

F_i's are permutations of $\mathbb{F}_{2^n}$, thus F is CCZ-equivalent to $F_2 \circ F_1^{-1}$ which is an APN permutation.

Dillon's APN permutation

At the Fq9 conference (Dublin 2009), Dillon presented the construction of an APN permutation on $\mathbb{F}_{2^6}$.

Theorem (Browning, Dillon, McQuistan, Wolfe)

$x^3 + \zeta x^{24} + x^{10}$ *is CCZ-equivalent to an APN permutation.*

- Consider the simplex codes contained in $\mathscr{C}(F)$.
- From any disjoint pairs of these simplex codes we can obtain a permutation.
- In total we can obtain 512 permutations.

Dillon's APN permutation

For all the APN permutations we have that the degree of their components are

```
{* 3^^7, 4^^56 *}
```

and the Walsh spectrum of the single components is given by the multi-set

```
{*
        {* -16, -8^^22, 0^^12, 8^^26, 16^^3 *}^^21,
        {* -16^^2, -8^^20, 0^^12, 8^^28, 16^^2 *}^^21,
        {* -16^^3, -8^^18, 0^^12, 8^^30, 16 *}^^7,
        {* -16^^6, 0^^48, 16^^10 *}^^7,
        {* -8^^24, 0^^12, 8^^24, 16^^4 *}^^7
 *}
```

Classification results for the Dillon's APN permutation

In the CCZ-class of $x^3 + \zeta x^{24} + x^{10}$ we have:

- 13 EA-classes;
- 2 of them contain a permutation;
- 4 affine-classes containing a permutation.

Remark

Checking affine equivalence using the code $\mathscr{C}_3(F)$ permits to identify 3 classes. Using $\mathscr{C}_4(F)$ it is possible to identify all the 4 classes. With $\mathscr{C}_3(F)$ we cannot understand if a function is equivalent to its inverse or not.

The case of dimension 7 and 8

In dimension 7 there are 490 known APN functions. For dimension 8 there are 8180 known APN functions. [2]

For dimension 7 and 8 the procedure for obtaining the L_1s can be still implemented. However, checking EA-equivalence using the code equivalence seems to require to much time.

We can give an upper bound on the number of EA-classes counting the simplex codes in $\mathscr{C}(F)$.

---

[2] Yu, Yuyin, Mingsheng Wang, and Yongqiang Li, A matrix approach for constructing quadratic APN functions, Designs, codes and cryptography 73.2 (2014): 587-600

Table: CCZ-inequivalent APN functions over $\mathbb{F}_{2^7}$ given in [Edel, Pott (2009)][3]

N.	function	# EA-classes $\leq$
1	x^3	256
2	x^5	256
3	x^9	256
4	x^{13}	2
5	x^{57}	2
6	$x^{63}(inverse)$	2
7	$x^3 + tr(x^9)$	184
8	$x^{34} + x^{18} + x^5$	184

N.	function	# EA-classes $\leq$
9	$x^{20} + x^6 + x^3$	324
10	$x^{66} + x^{34} + x^{20} + x^{17} + x^3$	184
11	$x^{34} + x^{33} + x^{17} + x^3$	184
12	$x^{34} + x^{33} + x^{10} + x^5 + x^3$	296
13	$x^{66} + x^{18} + x^9 + x^3$	212
14	$x^{33} + x^{17} + x^{12} + x^3$	240
15	$x^{66} + x^{34} + x^{20} + x^3$	184
16	$x^{72} + x^{40} + x^{12} + x^3$	184
17	$x^{72} + x^{40} + x^{34} + x^6 + x^3$	184
18	$x^{34} + x^{33} + x^{12} + x^6 + x^5 + x^3$	240
19	$x^{72} + x^{40} + x^{34} + x^6 + x^3 +$ $\zeta^{27}(tr(\zeta^{20}x^3 + \zeta^{94}x^5 + \zeta^{66}x^9))$	216

[3] Y. Edel, and A. Pott, A new almost perfect nonlinear function which is not quadratic. Adv. in Math. of Comm. 3.1 (2009): 59-81.

Table: CCZ-inequivalent APN functions over $\mathbb{F}_{2^8}$ given in [Edel, Pott (2009)].

N.	function	# EA-classes $\leq$
1	x^3	256
2	x^9	256
3	x^{57}	1
4	$\zeta^{15}x^{48}+\zeta^{16}x^{33}+\zeta^{16}x^{18}+x^{17}+x^3$	256
5	$x^3+Tr(x^9)$	256
6	$x^9+Tr(x^3)$	256
7	$\zeta^{21}x^{144}+\zeta^{183}x^{66}+\zeta^{245}x^{33}+x^3$	256
8	$\zeta^{135}x^{144}+\zeta^{120}x^{66}+\zeta^{65}x^{18}+x^3$	256
9	$\zeta^{67}x^{192}+\zeta^{182}x^{132}+\zeta^{24}x^6+x^3$	256
10	$x^{160}+x^{132}+x^{80}+x^{68}+x^6+x^3$	464
11	$x^{66}+x^{40}+x^{18}+x^5+x^3$	368
12	$x^{130}+x^{66}+x^{40}+x^{12}+x^3$	400

N.	function	# EA-classes $\leq$
13	$\zeta^{189}x^{192}+\zeta^{143}x^{144}+\zeta^{22}x^{132}+\zeta^{21}x^{129}+\zeta^{133}x^{96}+\zeta^{239}x^{72}+\zeta^{229}x^{66}+\zeta^{31}x^{48}+$ $\zeta^{187}x^{36}+\zeta^{185}x^{33}+\zeta^{68}x^{24}+\zeta^{236}x^{18}+\zeta^{75}x^{12}+\zeta^{91}x^9+\zeta^{97}x^6+\zeta^{160}x^3$	256
14	$\zeta^{100}x^{192}+\zeta^{12}x^{160}+\zeta^{15}x^{144}+\zeta^{243}x^{136}+\zeta^{234}x^{132}+\zeta^{33}x^{130}+\zeta^{39}x^{129}+\zeta^{139}x^{96}+$ $\zeta^{51}x^{80}+\zeta^{229}x^{72}+\zeta^{39}x^{68}+\zeta^{17}x^{66}+\zeta^{189}x^{65}+\zeta^{126}x^{48}+\zeta^{198}x^{40}+\zeta^{238}x^{36}+\zeta^{192}$ $x^{34}+\zeta^{217}x^{33}+\zeta^{122}x^{24}+\zeta^{144}x^{20}+\zeta^{169}x^{18}+\zeta^{141}x^{17}+\zeta^{236}x^{12}+$ $\zeta^{117}x^{10}+\zeta^{183}x^9+\zeta^{184}x^6+\zeta^{231}x^5+\zeta^{228}x^3$	400
15	$\zeta^{155}x^{192}+\zeta^{96}x^{144}+\zeta^{223}x^{132}+\zeta^{77}x^{129}+\zeta^{88}x^{96}+\zeta^{232}x^{72}+\zeta^{69}x^{66}+\zeta^{142}x^{48}+$ $\zeta^{168}x^{36}+x^{33}+\zeta^{145}x^{24}+\zeta^{234}x^{18}+\zeta^{202}x^{12}+\zeta^{94}x^9+\zeta^{189}x^6+\zeta^{241}x^3$	256
16	$\zeta^{126}x^{192}+\zeta^{119}x^{144}+\zeta^{221}x^{132}+\zeta^{222}x^{129}+\zeta^{79}x^{96}+\zeta^{221}x^{72}+\zeta^{187}x^{66}+$ $\zeta^{148}x^{48}+\zeta^{187}x^{36}+\zeta^{237}x^{24}+\zeta^{231}x^{12}+\zeta^{119}x^9+\zeta^{244}x^6+\zeta^{236}x^3$	256
17	$\zeta^{151}x^{192}+\zeta^{13}x^{144}+\zeta^{58}x^{132}+\zeta^{143}x^{129}+\zeta^{110}x^{96}+\zeta x^{72}+\zeta^{244}x^{66}+\zeta^{26}x^{48}+$ $\zeta^{180}x^{36}+\zeta^{8}x^{33}+\zeta^{69}x^{24}+\zeta^{76}x^{18}+\zeta^{201}x^{12}+\zeta^{201}x^9+\zeta^{19}x^6+\zeta^{107}x^3$	256
18	$\zeta^{86}x^{192}+\zeta^{224}x^{129}+\zeta^{163}x^{96}+\zeta^{102}x^{66}+\zeta^{129}x^{48}+\zeta^{102}x^{36}+\zeta^{170}x^{33}+$ $\zeta^{14}x^{24}+\zeta^{170}x^{18}+\zeta^{101}x^{12}+\zeta^{58}x^6+\zeta^{254}x^3$	256
19	$\zeta^{95}x^{192}+\zeta^{242}x^{144}+\zeta^{195}x^{132}+\zeta^{98}x^{129}+\zeta^{84}x^{96}+\zeta^{45}x^{72}+\zeta^{234}x^{66}+\zeta^{202}x^{48}+$ $\zeta^{159}x^{36}+\zeta^{58}x^{33}+\zeta^{23}x^{24}+\zeta^{148}x^{18}+\zeta^{230}x^{12}+\zeta^{32}x^9+\zeta^{54}x^6+\zeta^{41}x^3$	256
20	$\zeta^{132}x^{192}+\zeta^{37}x^{144}+\zeta^{91}x^{132}+\zeta^{188}x^{129}+\zeta^{76}x^{96}+\zeta^{162}x^{72}+\zeta^{46}x^{66}+\zeta^{252}x^{48}+$ $\zeta^{42}x^{36}+\zeta^{81}x^{33}+\zeta^{83}x^{24}+\zeta^{13}x^{18}+\zeta^{185}x^{12}+\zeta^{163}x^9+\zeta^{216}x^6+\zeta^{181}x^3$	256
21	$\zeta^{91}x^{192}+\zeta^{124}x^{144}+\zeta^{214}x^{132}+\zeta^{106}x^{129}+\zeta^{59}x^{96}+\zeta^{172}x^{72}+\zeta^{138}x^{66}+$ $\zeta^{163}x^{48}+\zeta^{58}x^{36}+\zeta^{100}x^{33}+\zeta^{32}x^{24}+\zeta^{250}x^{18}+\zeta^{45}x^{12}+\zeta^{241}x^6+\zeta^{157}x^3$	256
22	$\zeta^{25}x^{192}+\zeta^{140}x^{144}+\zeta^{59}x^{132}+\zeta^{129}x^{129}+\zeta^{42}x^{96}+\zeta^{164}x^{72}+\zeta^{149}x^{66}+\zeta^{119}x^{48}+$ $\zeta^{74}x^{36}+\zeta^{211}x^{33}+\zeta^{9}x^{24}+\zeta^{46}x^{18}+\zeta^{130}x^{12}+\zeta^{185}x^9+\zeta^{147}x^6+\zeta^{27}x^3$	256
23	$\zeta^{113}x^{192}+\zeta^{56}x^{144}+\zeta^{68}x^{132}+\zeta^{155}x^{129}+\zeta^{91}x^{96}+\zeta^{78}x^{72}+\zeta^{159}x^{66}+\zeta^{30}x^{48}+$ $\zeta^{194}x^{36}+\zeta^{14}x^{33}+\zeta^{238}x^{24}+\zeta^{91}x^{18}+\zeta^{100}x^{12}+\zeta^{96}x^9+\zeta^{222}x^6+\zeta^{178}x^3$	256

The case of non-Gold APN power functions and the inverse function

Table: Over $\mathbb{F}_{2^7}$.

N.	function	upper bound	# EA-classes
1	x^{13}	2	2
2	x^{57}	2	1
3	$x^{63}(inverse)$	2	1

Table: Over $\mathbb{F}_{2^8}$.

N.	function	upper bound	# EA-classes
1	x^{57}	1	1
2	$x^{127}(inverse)$	2	1

Table: Over $\mathbb{F}_{2^9}$.

N.	function	upper bound	# EA-classes
1	x^{13}	2	2
2	x^{19}	2	2
3	x^{241}	2	2
4	$x^{255}(inverse)$	2	1

Theorem

Let $n \leq 9$ and $F(x) = x^d$ be a non-Gold APN function defined over $\mathbb{F}_{2^n}$. Then the CCZ-class of F is partitioned in at most two EA-classes represented by F and F^{-1} (when exists).

Theorem (Li, Wang)

Let $n \geq 5$. The inverse function is EA-equivalent to a permutation if and only if it is affine equivalent to it.

Theorem

Let $5 \leq n \leq 9$. A permutation polynomial F defined over $\mathbb{F}_{2^n}$ is CCZ-equivalent to x^{-1} if and only if F is affine-equivalent to x^{-1}.

Thanks for your attention!