On relations between CCZ and EA-equivalences

Marco Calderini
(joint work with Lilya Budaghyan and Irene Villa)

University of Bergen

Boolean Functions and their Applications
June 17-22, 2018

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

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

The nonlinearity equals:

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

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 **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.

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 $\mathcal{L}$ an affine permutation on $(\mathbb{F}_{2^n})^2$, $\mathcal{L}(\Gamma_F) = \Gamma_G$.
EA and CCZ-equivalence preserve the nonlinearity and the differential uniformity.

CCZ-equivalence

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

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

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

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

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

EA-equivalence $\subset$ CCZ-equivalence

EA$\Rightarrow$ CCZ:

- If $(L_1(x,y), L_2(x,y)) = (x, A(x)+y)$ then $\mathcal{L}(x, F(x)) = (x, F(x)+A(x))$ and $G(x) = F(x)+A(x)$.
- If $(L_1(x,y), L_2(x,y)) = (A(x), y)$ then $\mathcal{L}(x, F(x)) = (A(x), F(x))$ and $G(x) = F \circ A^{-1}(x)$.
- If $(L_1(x,y), L_2(x,y)) = (x, A(y))$ then $\mathcal{L}(x, F(x)) = (x, A \circ F(x))$ and $G(x) = A \circ F(x)$.

inversion is a particular case of CCZ:

- $(L_1(x,y), L_2(x,y)) = (y, x)$ then $\mathcal{L}(x, F(x)) = (F(x), x)$ and $G(x) = F^{-1}(x)$.

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 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 $m \geq 2$.

EA-equivalence preserves algebraic degree while inverse and CCZ-equivalence do not.

Relation between CCZ and EA-equivalence + Inverse

Proposition (L. Budaghyan, C. Carlet, A. Pott)

G is EA-equivalent to the function F or to F^{-1} (if it exists) iff there exists a linear permutation $\mathcal{L} = (L_1, L_2)$ on $(\mathbb{F}_{2^n})^2$ such that $\mathcal{L}(\Gamma_F) = \Gamma_G$ and $L_1(x, y) = L(x)$ or $L_1(x, y) = L(y)$.

Relation between CCZ and EA-equivalence + Inverse

Proposition (L. Budaghyan, C. Carlet, A. Pott)

G is EA-equivalent to the function F or to F^{-1} (if it exists) iff there exists a linear permutation $\mathcal{L} = (L_1, L_2)$ on $(\mathbb{F}_{2^n})^2$ such that $\mathcal{L}(\Gamma_F) = \Gamma_G$ and $L_1(x, y) = L(x)$ or $L_1(x, y) = L(y)$.

If we want to construct G which cannot be constructed from F via EA-equivalence and inverse transformation:

- To find a permutation $L_1(x, F(x)) = L(x) + R \circ F(x)$ where $L, R \neq 0$ are linear.
- Then find linear function $L_2(x, y) = L'(x) + R'(y)$such that $\mathcal{L}$ is a permutation. (Found L_1 then there always exists suitable L_2)

Fixed L_1 , differents L' and R' produce EA-equivalent functions.

The condition that L_1 depends on both variables is necessary but not sufficient.

Example: Let $n = 2m + 1$ and $s = m \mod 2$. Then

$$\mathcal{L}(x, y) = (x + tr(x) + \sum_{i=0}^{m-s} y^{2^{2j}+s}, y + tr(x))$$

is a linear permutation and maps the graph of $F(x) = x^3$ to the graph of G which is EA-equivalent to F^{-1}.

CCZ-equivalence more general than EA-equivalence with inverse transformation

APN functions CCZ-equivalent to Gold functions and EA-inequivalent to power functions on $\mathbb{F}_{2^n}$

Function	conditions
$x^{2^i+1} + (x^{2^i} + x + tr(1) + 1)tr(x^{2^i} + 1 + xtr(1))$	$n \geq 4$, $\gcd(n,i) = 1$
$[x + tr_3^n(x^{2(2^i+1)} + x^{4(2^i+1)}) + tr(x)tr_3^n(x^{2^i+1} + x^{2^{2i}(2^i+1)})]^{2^i+1}$	$6 \mid n$, $\gcd(n,i) = 1$
$x^{2^i+1} + tr_m^n(x^{2^i+1}) + x^{2^i}tr_m^n(x) + xtr_m^n(x)^{2^i}$ $+[tr_m^n(x)^{2^i+1} + tr_m^n(x^{2^i+1}) + tr_m^n(x)]^{1/(2^i+1)}](x^{2^i} + tr_m^n(x^{2^i}) + 1)$ $+[tr_m^n(x)^{2^i+1} + tr_m^n(x^{2^i+1}) + tr_m^n(x)]^{2^i/(2^i+1)}](x + tr_m^n(x)+)$	n odd, $m \mid n$ $\gcd(n,i) = 1$

Only for Gold functions it is known that CCZ>EA+inverse. For the rest of power functions it is an open problem.

A procedure for investigating if $CCZ \stackrel{?}{=} EA + Inv$

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

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

$$\Downarrow$$

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

(L^* is the adjoint operator)

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

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

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 $\{u_1, \ldots, u_k\}$ 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 $\{u_1, \ldots, u_k\}$ of U we can suppose that

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

Construction of L^*

For any $a_1, \ldots, a_k$ with $a_1 \in \mathcal{ZW}(u_1), \ldots, a_k \in \mathcal{ZW}(u_k)$ we need to check if

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

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

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

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

Then,

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

Proposition

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 $\mathrm{Im}(R^*) = U$ iff the procedure above is successful.

Proposition

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 $\mathrm{Im}(R^*) = U$ iff the procedure above is successful.

Proposition

Let F be a a function from $\mathbb{F}_{2^n}$ to itself. If for any vector subspace $U \neq \{0\}$ in S_F is not possible to construct any matrix $L^* \neq 0$ with the previous procedure, then any function F' CCZ-equivalent to F can be obtained from F applying only the EA-equivalence and inverse transformation iteratively.

Application to non-quadratic functions

Let $n = 6$, and $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be

$$
\begin{aligned}
F(x) = & x^3 + u^{17}(x^{17} + x^{18} + x^{20} + x^{24}) \\
& + u^{14}((u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{11} + u^2x^{13}) + \\
& (u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{1}1 + u^2x^{13})^2 \\
& + (u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{1}1 + u^2x^{13})^4 + \\
& (u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{1}1 + u^2x^{13})^8 \\
& + (u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{1}1 + u^2x^{13})^{16} + \\
& (u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{1}1 + u^2x^{13})^{32} \\
& + (u^2x)^9 + (u^2x)^{18} + (u^2x)^{36} + x^{21} + x^{42}),
\end{aligned}
$$

where u is a primitive element of $\mathbb{F}_{2^n}$.

F is the first example of APN function CCZ-inequivalent to a quadratic function.

Using the procedure it is possible to construct the functions L and R given by

$$L(x) = u^{50}x^{32} + u^{51}x^{16} + u^{43}x^{8} + ux^{4} + u^{26}x^{2} + u^{26}x$$

and

$$R(x) = u^{26}x^{32} + u^{17}x^{16} + u^{56}x^{8} + u^{9}x^{4} + u^{54}x^{2} + u^{46}x,$$

Considering the function $F_2(x) = L_2(x, F(x)) = F(x)$
we have

$$\begin{aligned}
F'(x) =& u^{41}x^{60} + u^{29}x^{58} + u^{46}x^{57} + u^{3}x^{56} + u^{39}x^{54} + u^{47}x^{53} \\
& + u^{3}x^{52} + u^{62}x^{51} + u^{54}x^{50} + u^{62}x^{49} + u^{53}x^{48} + u^{14}x^{46} \\
& + u^{39}x^{45} + u^{20}x^{44} + u^{26}x^{43} + u^{11}x^{42} + u^{31}x^{41} + u^{53}x^{40} \\
& + u^{59}x^{39} + u^{53}x^{38} + u^{41}x^{37} + u^{19}x^{36} + u^{58}x^{35} + u^{2}x^{34} + \\
& u^{7}x^{33} + u^{39}x^{32} + u^{15}x^{30} + u^{17}x^{29} + u^{45}x^{28} + u^{39}x^{27} \\
& + u^{57}x^{26} + u^{33}x^{25} + u^{61}x^{24} + u^{41}x^{23} + u^{50}x^{22} + u^{58}x^{21} \\
& + u^{55}x^{20} + u^{26}x^{19} + u^{17}x^{18} + u^{37}x^{17} + u^{30}x^{16} + ux^{15} \\
& + u^{46}x^{14} + u^{21}x^{13} + u^{13}x^{12} + u^{61}x^{11} + u^{20}x^{10} + x^{9} + u^{61}x^{8}
\end{aligned}$$

The function F' cannot be constructed from F via EA-equivalence and inverse transformation.
F has algebraic degree equals to 3 and F' equals to 4.
Moreover to apply the inverse transformation at least once we need $F \sim_{EA} G$ with G permutation, but since F has quadratic components this cannot be possible.

Then we have that CCZ$>$EA$+$inversion also for APN functions inequivalent to quadratic functions

Note: F has quadratics components, that may be useful to crate the function F_1.

APN power functions

Power functions

Let $n = 7$ and $F(x) = x^d$ with d not a Gold exponent, i,e, $d = 11, 13, 39, 57, 126$. Then, in these cases the CCZ-equivalence coincide with the EA-equivalence and the inverse transformation.

Let $n = 8$ and $F(x) = x^{57}$ (Kasami). Then in this case the CCZ-equivalence coincide with the EA-equivalence and the inverse transformation.

EA-equivalence to a permutation

If $S_F = \mathbb{F}_{2^n}$ we can check if F is EA-equivalent to a permutation.

Theorem (Y. Li, M. Wang)

Suppose $F(x) = x^{2^i+1}$, *with* $\gcd(i, n) = 1$ *and* $L(x)$ *is a linearized polynomial on* $\mathbb{F}_{2^n}$. *Then* $F(x) + L(x)$ *is a permutation polynomial iff* n *is odd and* $L(x) = \alpha^{2^i} x + \alpha x^{2^i}$ *for some* $\alpha \neq 0$.

Theorem (Y. Li, M. Wang)

$x^{-1} + L(x)$ *is not a permutation on* $\mathbb{F}_{2^n}$ *whenever* $L \neq 0$ *when* $n \geq 5$.

Proposition

All known APN functions, except the Gold cases, for $n = 7, 9, 11$ are such that $F(x) + L(x)$ is not a permutation on $\mathbb{F}_{2^n}$ whenever $L \neq 0$. Moreover, $F(x) = x^3 + Tr(x^9)$ is not CCZ-equivalent to a permutation over $\mathbb{F}_{2^7}$.

Classification of APN functions

APN polynomial families CCZ-inequivalent to power functions

N°	Functions	Conditions
C1-C2	$x^{2^s+1} + u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n = pk$, $\gcd(k,p)$=$\gcd(s,pk)$=1, $p \in \{3,4\}$, $i = sk \bmod p$, $m = p - i$, $n \geq 12$, u primitive in $\mathbb{F}_{2^n}^*$
C3	$x^{2^{2i}+2^i} + cx^{q+1} + dx^{q(2^{2i}+2^i)}$	$q = 2^m$, $n = 2m$, $\gcd(i,m)$=1, $\gcd(2^i+1, q+1) \neq 1$, $dc^q + c \neq 0$, $d \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^n}\}$, $d^{q+1} = 1$
C4	$x(x^{2^i} + x^q + cx^{2^iq})$ $+x^{2^i}(c^qx^q + sx^{2^iq}) + x^{(2^i+1)q}$	$q = 2^m$, $n = 2m$, $\gcd(i,m)$=1, $c \in \mathbb{F}_{2^n}$, $s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$, $X^{2^i+1} + cX^{2^i} + c^qX + 1$ is irreducible over $\mathbb{F}_{2^n}$
C5	$x^3 + a^{-1}Tr(a^3x^9)$	$a \neq 0$
C6	$x^3 + a^{-1}Tr_n^3(a^3x^9 + a^6x^{18})$	$3\|n$, $a \neq 0$
C7	$x^3 + a^{-1}Tr_n^3(a^6x^{18} + a^{12}x^{36})$	$3\|n$, $a \neq 0$

Classification of APN functions

C8-C10	$ux^{2^s+1} + u^{2^k} x^{2^{-k}+2^{k+s}} +$ $vx^{2^{-k}+1} + wu^{2^k+1} x^{2^s+2^{k+s}}$	$n = 3k$, $\gcd(k,3)$=$\gcd(s,3k)$=1, $v, w \in \mathbb{F}_{2^k}$, $vw \neq 1$, $3 \mid (k+s)$ u primitive in $\mathbb{F}_{2^n}^*$
C11	$dx^{2^s+1} + d^{2^k} x^{2^{k+s}+2^k} +$ $cx^{2^k+1} + \sum_{i+1}^{k-1} \gamma_i x^{2^{k+i}+2^i}$	$n = 2k$, $\gcd(s,k)$=1, s, k odd, $c \notin \mathbb{F}_{2^k}$, $\gamma_i \in \mathbb{F}_{2^k}$, d not a cube
C12	$(x + x^{2^m})^{2^k+1} +$ $u'(ux + u^{2^m} x^{2^m})^{(2^k+1)2^i} +$ $u(x + x^{2^m})(ux + u^{2^m} x^{2^m})$	$n = 2m$, $m \geq 2$ even, $\gcd(k,m) = 1$ and i even u primitive in $\mathbb{F}_{2^n}^*$, $u' \in \mathbb{F}_{2^m}$ not cube
C13	$x^{2^k+1} + tr_m^n(x)^{2^k+1}$	$n = 2m = 4t$, $\gcd(k,n) = 1$
C14	$a^2 x^{2^{2m+1}+1} + b^2 x^{2^{m+1}+1} + ax^{2^{2m}+2}$ $+bx^{2^m+2} + (c^2+c)x^3$	$n = 3m$, m odd Irene Villa's talk

Classification of APN functions

C8-C10	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+$ $vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n=3k$, $\gcd(k,3)$=$\gcd(s,3k)$=1, $v,w\in\mathbb{F}_{2^k}$, $vw\neq 1$, $3\|(k+s)$ u primitive in $\mathbb{F}_{2^n}^*$
C11	$dx^{2^s+1}+d^{2^k}x^{2^{k+s}+2^k}+$ $cx^{2^k+1}+\sum_{i+1}^{k-1}\gamma_i x^{2^{k+i}+2^i}$	$n=2k$, $\gcd(s,k)$=1, s,k odd, $c\notin\mathbb{F}_{2^k}$, $\gamma_i\in\mathbb{F}_{2^k}$, d not a cube
C12	$(x+x^{2^m})^{2^k+1}+$ $u'(ux+u^{2^m}x^{2^m})^{(2^k+1)2^i}+$ $u(x+x^{2^m})(ux+u^{2^m}x^{2^m})$	$n=2m$, $m\geq 2$ even, $\gcd(k,m)=1$ and i even u primitive in $\mathbb{F}_{2^n}^*$, $u'\in\mathbb{F}_{2^m}$ not cube
C13	$x^{2^k+1}+tr_m^n(x)^{2^k+1}$	$n=2m=4t$, $\gcd(k,n)=1$
C14	$a^2x^{2^{2m+1}+1}+b^2x^{2^{m+1}+1}+ax^{2^{2m}+2}$ $+bx^{2^m+2}+(c^2+c)x^3$	$n=3m$, m odd Irene Villa's talk

C13 is equivalent to $x^{2^{m-k}+1}$ (L. Budaghyan, T. Helleseth, N. Li, B. Sun)

C3, C4 and C11

C3	$x^{2^{2i}+2^i} + cx^{q+1} + dx^{q(2^{2i}+2^i)}$	$q = 2^m$, $n = 2m$, $\gcd(i, m)$=1, $\gcd(2^i + 1, q + 1) \neq 1$, $dc^q + c \neq 0$, $d \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^n}\}$, $d^{q+1} = 1$
C4	$x(x^{2^i} + x^q + cx^{2^i q})$ $+x^{2^i}(c^q x^q + sx^{2^i q}) + x^{(2^i+1)q}$	$q = 2^m$, $n = 2m$, $\gcd(i, m)$=1, $c \in \mathbb{F}_{2^n}$, $s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$, $X^{2^i+1} + cX^{2^i} + c^q X + 1$ is irreducible over $\mathbb{F}_{2^n}$
C11	$dx^{2^s+1} + d^{2^k} x^{2^{k+s}+2^k} +$ $cx^{2^k+1} + \sum_{i=1}^{k-1} \gamma_i x^{2^{k+i}+2^i}$	$n = 2k$, $\gcd(s, k)$=1, s, k odd, $c \notin \mathbb{F}_{2^k}$, $\gamma_i \in \mathbb{F}_{2^k}$, d not a cube

C3⊆C11

$n = 2k$, $q = 2^k$

$$F(x) = cx^{q+1} + x^{2^{2i}+2^i} + dx^{q(2^{2i}+2^i)}$$

C3⊆C11

$n = 2k,\ q = 2^k$

$$F(x) = cx^{q+1} + x^{2^{2i}+2^i} + dx^{q(2^{2i}+2^i)}$$

$d^{q+1} = 1 \Rightarrow \exists d'$ s.t. $d = d'^{q-1}$

$$F'(x) = d'F(x) = d'cx^{q+1} + d'x^{2^{2i}+2^i} + d'^{q}x^{q(2^{2i}+2^i)}$$

C3⊆C11

$n = 2k, \; q = 2^k$

$$F(x) = cx^{q+1} + x^{2^{2i}+2^i} + dx^{q(2^{2i}+2^i)}$$

$d^{q+1} = 1 \Rightarrow \exists d'$ s.t. $d = d'^{q-1}$

$$F'(x) = d'F(x) = \underbrace{d'cx^{q+1}}_{d'c\mathbb{F}_q} + \underbrace{d'x^{2^{2i}+2^i} + d'^q x^{q(2^{2i}+2^i)}}_{\mathbb{F}_q}$$

$dc^q + c \neq 0 \Rightarrow d'c \notin \mathbb{F}_{2^k}$, so $\mathbb{F}_{2^n} = d'c\mathbb{F}_q \oplus \mathbb{F}_q$.

C3⊆C11

$n = 2k, \; q = 2^k$

$$F(x) = cx^{q+1} + x^{2^{2i}+2^i} + dx^{q(2^{2i}+2^i)}$$

$d^{q+1} = 1 \Rightarrow \exists d'$ s.t. $d = d'^{q-1}$

$$F'(x) = d'F(x) = \underbrace{d'cx^{q+1}}_{d'c\mathbb{F}_q} + \underbrace{d'x^{2^{2i}+2^i} + d'^q x^{q(2^{2i}+2^i)}}_{\mathbb{F}_q}$$

$dc^q + c \neq 0 \Rightarrow d'c \notin \mathbb{F}_{2^k}$, so $\mathbb{F}_{2^n} = d'c\mathbb{F}_q \oplus \mathbb{F}_q$. We can apply a linear permutation which is the identity on $d'c\mathbb{F}_q$ and $x^{1/2^i}$ on $\mathbb{F}_q$.

$$L \circ F'(x) = d'cx^{q+1} + d''x^{2^i+1} + d''^q x^{q(2^i+1)} \in C11$$

$d'' = d'^{1/2^i}$

It is possible to prove also that C11$\subseteq$C3

Lemma

C3=C11

C11⊆C4

$$F(x) = dx^{2^i+1} + d^q x^{q(2^i+1)} + cx^{q+1} + \sum_{s=1}^{k-1} \gamma_s x^{(q+1)2^s}$$

C11⊆C4

$$F(x) = dx^{2^i+1} + d^q x^{q(2^i+1)} + cx^{q+1} + \sum_{s=1}^{k-1} \gamma_s x^{(q+1)2^s}$$

Let $L(x) = (x + x^q)^{2^t} + w(x + x^q) + (c + c^q)^{2^t} x$

C11⊆C4

$$F(x) = dx^{2^i+1} + d^q x^{q(2^i+1)} + cx^{q+1} + \sum_{s=1}^{k-1} \gamma_s x^{(q+1)2^s}$$

Let $L(x) = (x + x^q)^{2^t} + w(x + x^q) + (c + c^q)^{2^t} x$
$w \in \mathbb{F}_q \Rightarrow L(x)$ permutation

$$\frac{L \circ F(x)}{(c + c^q)^{2^t}} = dx^{2^i+1} + d^q x^{q(2^i+1)} + c' x^{q+1} + \sum_{\substack{s=1 \\ s \neq t}}^{k-1} \gamma_s x^{(q+1)2^s}$$

$c' = w(c + c^q)^{1-2^t} + c.$

C11⊆C4

$$F(x) = dx^{2^i+1} + d^q x^{q(2^i+1)} + cx^{q+1} + \sum_{s=1}^{k-1} \gamma_s x^{(q+1)2^s}$$

Let $L(x) = (x + x^q)^{2^t} + w(x + x^q) + (c + c^q)^{2^t} x$
$w \in \mathbb{F}_q \Rightarrow L(x)$ permutation

$$\frac{L \circ F(x)}{(c + c^q)^{2^t}} = dx^{2^i+1} + d^q x^{q(2^i+1)} + c' x^{q+1} + \sum_{\substack{s=1 \\ s \neq t}}^{k-1} \gamma_s x^{(q+1)2^s}$$

$c' = w(c + c^q)^{1-2^t} + c.$
Wlog

$$F(x) = dx^{2^i+1} + d^q x^{q(2^i+1)} + cx^{q+1} + x^{(q+1)2^i}$$

Similarly

$$H(x) = \bar{d}x^{2^i(q+1)} + x^{(q+1)} + (x^{2^i+1} + x^{q(2^i+1)} + \bar{c}x^{q2^i+1} + \bar{c}^q x^{2^i+q})$$

is equivalent to

$$H'(x) = \bar{d}'x^{(q+1)} + (x^{2^i+1} + x^{q(2^i+1)} + \bar{c}x^{q2^i+1} + \bar{c}^q x^{2^i+q})$$

Similarly

$$H(x) = \bar{d}x^{2^i(q+1)} + x^{(q+1)} + (x^{2^i+1} + x^{q(2^i+1)} + \bar{c}x^{q2^i+1} + \bar{c}^q x^{2^i+q})$$

is equivalent to

$$H'(x) = \bar{d}'x^{(q+1)} + (x^{2^i+1} + x^{q(2^i+1)} + \bar{c}x^{q2^i+1} + \bar{c}^q x^{2^i+q})$$

We want to prove that $F(x) = dx^{2^i+1} + d^q x^{q(2^i+1)} + cx^{q+1} + x^{(q+1)2^i}$ is equivalent to $H'(x)$

Consider a permutation $x + \gamma x^q$ with $\gamma^{q+1} \neq 1$,

$$\begin{aligned} F(x+\gamma x^q) =& (c + c\gamma^{q+1})x^{q+1} + (1+\gamma^{2^i(q+1)})x^{2^i(q+1)} \\ &+ (d + d^{2^m}\gamma^{q(2^i+1)})x^{2^i+1} + (d^{2^m} + d\gamma^{2^i+1})x^{q(2^i+1)} \\ &+ (d\gamma^{2^i} + d^{2^m}\gamma^q)x^{q2^i+1} + (d^{2^m}\gamma^{q2^i} + d\gamma)x^{2^i+q} \\ &+ \text{terms of } \deg \leq 1 \end{aligned}$$

Consider a permutation $x + \gamma x^q$ with $\gamma^{q+1} \neq 1$,

$$\begin{aligned} F(x + \gamma x^q) = &(c + c\gamma^{q+1})x^{q+1} + (1 + \gamma^{2^i(q+1)})x^{2^i(q+1)} \\ &+ (d + d^{2^m}\gamma^{q(2^i+1)})x^{2^i+1} + (d^{2^m} + d\gamma^{2^i+1})x^{q(2^i+1)} \\ &+ (d\gamma^{2^i} + d^{2^m}\gamma^q)x^{q2^i+1} + (d^{2^m}\gamma^{q2^i} + d\gamma)x^{2^i+q} \\ &+ \text{terms of } \deg \leq 1 \end{aligned}$$

Which is EA-equivalent to

Consider a permutation $x + \gamma x^q$ with $\gamma^{q+1} \neq 1$,

$$\begin{aligned}
F(x + \gamma x^q) =& (c + c\gamma^{q+1})x^{q+1} + (1 + \gamma^{2^i(q+1)})x^{2^i(q+1)} \\
& + (d + d^{2^m}\gamma^{q(2^i+1)})x^{2^i+1} + (d^{2^m} + d\gamma^{2^i+1})x^{q(2^i+1)} \\
& + (d\gamma^{2^i} + d^{2^m}\gamma^q)x^{q2^i+1} + (d^{2^m}\gamma^{q2^i} + d\gamma)x^{2^i+q} \\
& + \text{terms of } \deg \leq 1
\end{aligned}$$

Which is EA-equivalent to

$$F'(x) = c'x^{q+1} + (ax^{2^i+1} + a^q x^{q(2^i+1)} + bx^{q2^i+1} + b^q x^{2^i+q}).$$

$a = (d + d^q\gamma^{q(2^i+1)})$ and $b = (d\gamma^{2^i} + d^q\gamma^q)$

Lemma

There exist $\gamma \in \mathbb{F}_{q^2}$ *and* $\delta \in \mathbb{F}_q$ *such that* $\gamma^{q+1} \neq 1$ *and* $\delta d \gamma^{2^i} + \delta d^q \gamma^q$ *is a* $2^i + 1$*th power.*

Lemma

There exist $\gamma \in \mathbb{F}_{q^2}$ and $\delta \in \mathbb{F}_q$ such that $\gamma^{q+1} \neq 1$ and $\delta d \gamma^{2^i} + \delta d^q \gamma^q$ is a $2^i + 1$th power.

$$\Downarrow$$

up to multiply F' by some $\delta \in \mathbb{F}_q$, there exist γ and $\lambda \neq 0$ such that $\lambda^{2^i+1} = (d + d^q \gamma^{q(2^i+1)})$ and substituting $x \mapsto \lambda^{-1} x$ we obtain

$$\bar{F}(x) = c'' x^{q+1} + x^{2^i+1} + x^{q(2^i+1)} + b'' x^{q2^i+1} + b''^q x^{2^i+q}.$$

Now, $c'' \notin \mathbb{F}_q$ and $\bar{F}$ APN imply that

$$x^{2^i+1} + b'' x^{2^i} + b''^q x + 1 = 0$$

has no solution x such that $x^{q+1} = 1$.

Now, $c'' \notin \mathbb{F}_q$ and $\bar{F}$ APN imply that

$$x^{2^i+1} + b''x^{2^i} + b''^q x + 1 = 0$$

has no solution x such that $x^{q+1} = 1$.

Theorem

$C3 = C11 \subseteq C4$.

Moreover we can rewrite the family of the hexanomials as:

$$H(x) = dx^{(q+1)} + (x^{2^i+1} + x^{q(2^i+1)} + cx^{q2^i+1} + c^q x^{2^i+q}).$$

Particular case: C12 with $i = 0$

When $i = 0$ for the family C12 we have that

$$F(x) = (x + x^q)^{2^k+1} + u'(ux + u^q x^q)^{2^k+1} + u(x + x^q)(ux + u^q x^q),$$

and it is possible to prove in a similar way that F is EA equivalent to $H(x)$ in the previous theorem.

Thanks for your attention!