Search for APN permutations among known APN functions

Jiří Pavlů

(joint work with Faruk Göloğlu)

Department of Algebra, Charles University in Prague

20 June 2019

Content of the talk

- APN functions – CCZ–equivalence to permutations.

Content of the talk

- APN functions – CCZ–equivalence to permutations.
- We provide computational proof of CCZ–inequivalence to a permutations for functions from known families up to dimension $\mathbb{F}_{2^{12}}$ (with a single known exception).

Content of the talk

- APN functions – CCZ–equivalence to permutations.
- We provide computational proof of CCZ–inequivalence to a permutations for functions from known families up to dimension $\mathbb{F}_{2^{12}}$ (with a single known exception).
- We show a new EA invariant for component–wise plateaued functions.

Content of the talk

- APN functions – CCZ–equivalence to permutations.
- We provide computational proof of CCZ–inequivalence to a permutations for functions from known families up to dimension $\mathbb{F}_{2^{12}}$ (with a single known exception).
- We show a new EA invariant for component–wise plateaued functions.
- We provide a proof of CCZ–inequivalence of $x^3 + \mathrm{Tr}(x^9)$ to a permutation in doubly even extensions.

Definitions

Definition (APN function)

Let f be a function on $\mathbb{F}_{2^n}$, we say that f is almost perfect nonlinear function, if for all $a \in \mathbb{F}_{2^n}^*$ and all $b \in \mathbb{F}_{2^n}$ the equation

$$f(x) + f(x+a) = b$$

has always either 0 or 2 solutions:

Definition (Trace)

Let $n > m$, $m|n$. Then we call the function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ such that:

$$\mathrm{tr}_m^n(\alpha) = \sum_{i=0}^{\frac{n}{m}-1} \alpha^{2^{mi}},$$

the *trace* function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$.

Definition

Walsh transform Let f be a function on $\mathbb{F}_{2^n}$. We call a function

$$\hat{f}(u,v) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(vf(x))+\mathrm{Tr}(ux)} = \sum_{x\in\mathbb{F}_{2^n}} \chi(vf(x)+ux)$$

the *Walsh transform* of f.

Definition

Walsh transform Let f be a function on $\mathbb{F}_{2^n}$. We call a function

$$\hat{f}(u,v) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(vf(x)) + \mathrm{Tr}(ux)} = \sum_{x \in \mathbb{F}_{2^n}} \chi(vf(x) + ux)$$

the *Walsh transform* of f.

$$\mathrm{Z}_f = \{(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} : \hat{f}(u,v) = 0\}$$

Definitions

Definition

Walsh transform Let f be a function on $\mathbb{F}_{2^n}$. We call a function

$$\hat{f}(u,v) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(vf(x)) + \mathrm{Tr}(ux)} = \sum_{x \in \mathbb{F}_{2^n}} \chi(vf(x) + ux)$$

the *Walsh transform* of f.

$$\mathrm{Z}_f = \{(u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} : \hat{f}(u,v) = 0\}$$

$$\mathrm{NB}_f = \{v \in \mathbb{F}_{2^n} : \hat{f}(0,v) \neq \pm 2^{n/2}\}$$

Notions of equivalence

Definition (Extended Affine (EA) equivalence)

Let f, g be functions on $\mathbb{F}_{2^n}$, we say that f is EA–equivalent to g if

$$g(x) = (L_1 \circ f \circ L_2)(x) + L_3(x)$$

for some L_1, L_2 affine permutations and L_3 affine function.

Definition (Carlet–Charpin–Zinoviev (CCZ) equivalence)

Let f, g be functions on $\mathbb{F}_{2^n}$, we say that f is CCZ–equivalent to g if there exists an affine mapping M such that

$$\{(x, f(x)), x \in \mathbb{F}_{2^n}\} = M(\{(x, g(x)), x \in \mathbb{F}_{2^n}\}).$$

Current state of knowledge

- We have one example of an APN permutation on $\mathbb{F}_{2^6}$.
(K.A. Browning, J.F. Dillon, M.T. McQuistan and A.J. Wolfe, 2010)

Current state of knowledge

- We have one example of an APN permutation on $\mathbb{F}_{2^6}$.
(K.A. Browning, J.F. Dillon, M.T. McQuistan and A.J. Wolfe, 2010)
- We have computational proof, that up to dimension 10 there is no other APN permutation among known APN functions.
(same paper)

Current state of knowledge

- We have one example of an APN permutation on $\mathbb{F}_{2^6}$.
(K.A. Browning, J.F. Dillon, M.T. McQuistan and A.J. Wolfe, 2010)
- We have computational proof, that up to dimension 10 there is no other APN permutation among known APN functions.
(same paper)
- We know, that in dimension 4 there are none. (e.g. M. Calderini, M. Sala and I. Villa, 2015)

Table: Known infinite families of APN multinomial functions on $\mathbb{F}_{2^{2n}}$

#	Polynomial	Conditions
1	$X^{2^s+1} + A^{2^t-1}X^{2^{it}+2^{rt+s}}$	$n = 3t,\ \gcd(t,3) = \gcd(s,3t) = 1$ $t \geq 3,\ i \equiv st \pmod 3,\ r = 3-i,$ $A \in \mathbb{F}$ is primitive
2	$X^{2^s+1} + A^{2^t-1}X^{2^{it}+2^{rt+s}}$	$n = 4t,\ \gcd(t,2) = \gcd(s,2t) = 1$ $t \geq 3,\ i \equiv st \pmod 4,\ r = 4-i,$ $A \in \mathbb{F}$ is primitive
3	$AX^{2^s+1} + A^{2^m}X^{2^{m+s}+2^m} + BX^{2^m+1} + \sum_{i=1}^{m-1} c_i X^{2^{m+i}+2^i}$	$n = 2m,\ m$ odd, $c_i \in \mathbb{F}_{2^m},$ $\gcd(s,m) = 1,\ s$ odd, $A, B \in \mathbb{F}$ is primitive
4	$AX^{2^{n-t}+2^{t+s}} + A^{2^t}X^{2^s+1} + bX^{2^{t+s}+2^s}$	$n = 3t,\ \gcd(t,3) = \gcd(s,3t) = 1,$ $3 \mid t+s,\ A \in \mathbb{F}$ is primitive, $b \in \mathbb{F}_{2^t}$
5	$A^{2^t}X^{2^{n-t}+2^{t+s}} + AX^{2^s+1} + bX^{2^{n-t}+1}$	$n = 3t,\ \gcd(t,3) = \gcd(s,3t) = 1,$ $3 \mid t+s,\ A \in \mathbb{F}$ is primitive, $b \in \mathbb{F}_{2^t}$
6	$A^{2^t}X^{2^{n-t}+2^{t+s}} + AX^{2^s+1} + bX^{2^{n-t}+1} + cA^{2^t+1}X^{2^{t+s}+2^s}$	$n = 3t,\ \gcd(t,3) = \gcd(s,3t) = 1,$ $3 \mid t+s,\ A \in \mathbb{F}$ is primitive, $b, c \in \mathbb{F}_{2^t},\ bc \neq 1$
7	$X^{2^{2k}+2^k} + BX^{q+1} + CX^{q(2^{2k}+2^k)}$	$n = 2m,\ m$ odd, C is a $(q-1)$st power but not a $(q-1)(2^i+1)$st power, $CB^q \neq B$
8	$X(X^{2^k} + X^q + CX^{2^k q}) + X^{2^k}(C^q X^q + AX^{2^k q}) + X^{(2^k+1)q}$	$n = 2m,\ \gcd(n,k) = 1,$ C satisfies $X^{2^i+1} + CX^{2^i} + C^{2^{n/2}}X + 1$ is irreducible, $A \in \mathbb{F} \backslash \mathbb{F}_{2^m}$
9	$X^3 + a^{-1}\mathrm{tr}_1^n(a^3X^9)$	

Dillon's approach

Theorem

A function f is CCZ–equivalent to a permutation if and only if there exist spaces U, V in $Z_f \bigcup \{(0,0)\}$, such that $U \bigcap V = \{(0,0)\}$ and $dim(U) = dim(V) = n$.

Note that this is an if–and–only–if condition.

Our approach

Theorem

If a component–wise plateaued function f is CCZ–equivalent to a permutation, then there must exist subspaces U, V in NB_f such that $U^{\perp} \bigcap V^{\perp} = \{0\}$ (i.e. $U + V = \mathbb{F}$). In particular $dim(U) + dim(V) \geq n$.

Our approach

Theorem

If a component–wise plateaued function f is CCZ–equivalent to a permutation, then there must exist subspaces U, V in NB_f such that $U^\perp \bigcap V^\perp = \{0\}$ (i.e. $U + V = \mathbb{F}$). In particular $dim(U) + dim(V) \geq n$.

Corollary

If a component–wise plateaued function f is CCZ–equivalent to a function, then there must exist a subspace in NB_f of dimension $n/2$.

Note that none of these is an if–and–only–if condition.

Speed

- Standard approach basically searches Z_f ($|\mathrm{Z}_f| \approx 2^{4m-2}$) for two trivially intersecting subspaces of dimension n.

Speed

- Standard approach basically searches Z_f ($|\mathrm{Z}_f| \approx 2^{4m-2}$) for two trivially intersecting subspaces of dimension n.
- Our approach only requires searching for two trivially intersecting subspaces of dimension $n/2$ in NB_f. It is known, that for component–wise plateaued APN functions we have $|\mathrm{NB}_f| < \sqrt{|\mathrm{Z}_f|}$ – therefore this approach is faster both practically and asymptotically.

Theorem (EA Invariant)

Let f and g be EA–equivalent, which are both plateaued. Let N_i and M_i denote the numbers of i–dimensional subspaces in NB_f and NB_g respectively. Then $N_i = M_i$ for every $i \in \mathbb{N}$.

EA Invariant

Theorem (EA Invariant)

Let f and g be EA–equivalent, which are both plateaued. Let N_i and M_i denote the numbers of i–dimensional subspaces in NB_f and NB_g respectively. Then $N_i = M_i$ for every $i \in \mathbb{N}$.

As it is known, that for quadratic APN functions the EA and CCZ equivalence coincide (Yoshiara, 2011) it follows, that for these functions it is even a CCZ invariant.

Proof.

Let $g = L_1(f(L_2(x))) + L_3(x)$.

$$\hat{g}(0,\alpha) = \sum_{x\in\mathbb{F}} \chi(\alpha g(x)) = \sum_{x\in\mathbb{F}} \chi(\alpha(L_1 \circ f \circ L_2(x)) + \alpha L_3(x))$$

Proof.

Let $g = L_1(f(L_2(x))) + L_3(x)$.

$$\hat{g}(0,\alpha) = \sum_{x\in\mathbb{F}} \chi(\alpha g(x)) = \sum_{x\in\mathbb{F}} \chi(\alpha(L_1 \circ f \circ L_2(x)) + \alpha L_3(x))$$

Rewrite using L^* as the adjoint mapping to L, and $x = L_2^{-1}(y)$:

$$\sum_{x\in\mathbb{F}} \chi(f(y)L_1^*(\alpha) + y(L_3 \circ L_2^{-1})^*(\alpha)) = \hat{f}((L_3 \circ L_2^{-1})^*(\alpha), L_1^*(\alpha)).$$

EA Invariant

Proof.
Let $g = L_1(f(L_2(x))) + L_3(x)$.

$$\hat{g}(0,\alpha) = \sum_{x\in\mathbb{F}} \chi(\alpha g(x)) = \sum_{x\in\mathbb{F}} \chi(\alpha(L_1 \circ f \circ L_2(x)) + \alpha L_3(x))$$

Rewrite using L^* as the adjoint mapping to L, and $x = L_2^{-1}(y)$:

$$\sum_{x\in\mathbb{F}} \chi(f(y)L_1^*(\alpha) + y(L_3 \circ L_2^{-1})^*(\alpha)) = \hat{f}((L_3 \circ L_2^{-1})^*(\alpha), L_1^*(\alpha)).$$

f and g are plateaued. Therefore supposing $\alpha \in \mathrm{NB}_g$ ($\hat{g}(0,\alpha) \neq \pm 2^{n/2}$), we have that

$$\hat{f}((L_3 \circ L_2^{-1})^*(\alpha), L_1^*(\alpha)) \neq \pm 2^{n/2} \Leftrightarrow \hat{f}((0, L_1^*(\alpha)) \neq \pm 2^{n/2}.$$

EA Invariant

Proof.
Let $g = L_1(f(L_2(x))) + L_3(x)$.

$$\hat{g}(0,\alpha) = \sum_{x\in\mathbb{F}} \chi(\alpha g(x)) = \sum_{x\in\mathbb{F}} \chi(\alpha(L_1 \circ f \circ L_2(x)) + \alpha L_3(x))$$

Rewrite using L^* as the adjoint mapping to L, and $x = L_2^{-1}(y)$:

$$\sum_{x\in\mathbb{F}} \chi(f(y)L_1^*(\alpha) + y(L_3 \circ L_2^{-1})^*(\alpha)) = \hat{f}((L_3 \circ L_2^{-1})^*(\alpha), L_1^*(\alpha)).$$

f and g are plateaued. Therefore supposing $\alpha \in \mathrm{NB}_g$ ($\hat{g}(0,\alpha) \neq \pm 2^{n/2}$), we have that

$$\hat{f}((L_3 \circ L_2^{-1})^*(\alpha), L_1^*(\alpha)) \neq \pm 2^{n/2} \Leftrightarrow \hat{f}((0, L_1^*(\alpha)) \neq \pm 2^{n/2}.$$

Therefore every $U \subseteq \mathrm{NB}_g$ is mapped to $L_1^*(U) \subseteq \mathrm{NB}_f$. □

Results

- For $\mathbb{F}_{2^{12}}$ all functions of all known (to authors) families were proven not to be CCZ–equivalent to a permutation.

Results

- For $\mathbb{F}_{2^{12}}$ all functions of all known (to authors) families were proven not to be CCZ–equivalent to a permutation.
- Partial CCZ–inequivalence results were found for some function families.

Results

Table: Calculated maximal dimensions of subspaces in NB_f

#	$n = 6$	$n = 8$	$n = 10$	$n = 12$
1	-	-	-	4 (3)
2	-	-	-	4
3	2	-	4	-
4	$3^\dagger$	-	-	4 (3)
5	$3^\dagger$	-	-	4
6	$3^\dagger$	-	-	3
7	2	-	4	-
8	2	2	4	3
9	3°	3	$5^{\circ\circ}$	4

"$\dagger$" – in this family in this dimension there are functions which are equivalent to the Dillon's APN permutation.
"$\circ$" – is just x^3 which is not CCZ–equivalent to a permutation.
"$\circ\circ$" – only one subspace of the stated dimension – $\mathbb{F}_q$.

Table: Currently known results on CCZ–inequivalence to permutations for APN function classes

	$n = 4k$	$n = 4k + 2$	
Gold	✓	✓	F. Göloğlu and P. Langevin
Kasami	✓	?	F. Göloğlu and P. Langevin
$x^3 + \mathrm{Tr}(x^9)$	✓	?	here
Dobbertin	?	?	

Results

Theorem

Let $\mathbb{F} = \mathbb{F}_{q^2}$, $q = 2^m$, m even. Then $x^3 + Tr(x^9)$ is not CCZ–equivalent to a permutation on $\mathbb{F}$.

For the proof we will require the following lemmata. From now on $C = \{a^3 : a \in \mathbb{F}^*\}$.

Lemma (Carlitz)

$$\sum_{x \in \mathbb{F}} \chi(ax^3) = \begin{cases} q^2 & \text{if } a = 0 \\ (-1)^{m+1} 2q & \text{if } a \in C \\ (-1)^m q & \text{if } a \notin C \end{cases}$$

For the proof we will require the following lemmata. From now on $C = \{a^3 : a \in \mathbb{F}^*\}$.

Lemma (Carlitz)

$$\sum_{x\in\mathbb{F}} \chi(ax^3) = \begin{cases} q^2 & \text{if } a = 0 \\ (-1)^{m+1}2q & \text{if } a \in C \\ (-1)^m q & \text{if } a \notin C \end{cases}$$

Lemma (Göloğlu and Langevin)

Let $\mathbb{F}_{2^{2m}}$, m even. Then there is no subspace in C of dimension m.

For the proof we will require the following lemmata. From now on $C = \{a^3 : a \in \mathbb{F}^*\}$.

Lemma (Carlitz)

$$\sum_{x \in \mathbb{F}} \chi(ax^3) = \begin{cases} q^2 & \text{if } a = 0 \\ (-1)^{m+1} 2q & \text{if } a \in C \\ (-1)^m q & \text{if } a \notin C \end{cases}$$

Lemma (Göloğlu and Langevin)

Let $\mathbb{F}_{2^{2m}}$, m even. Then there is no subspace in C of dimension m.

Lemma

Let $\mathbb{F}_{2^{2m}}$, m even. Then there for every $(m-1)$–dimensional subspace V in C it holds that $|V^{\perp} \bigcap C| = 1$.

Proof of the last lemma

Consider $\sum_{v \in V} \sum_{x \in \mathbb{F}} \chi(vx^3)$, and sum it in two ways.

Proof of the last lemma

Consider $\sum_{v\in V}\sum_{x\in\mathbb{F}}\chi(vx^3)$, and sum it in two ways.

$$q^2 - 2q(\frac{q}{2}-1) = \sum_{v\in V}\sum_{x\in\mathbb{F}}\chi(vx^3) = \frac{q}{2}(3|V^\perp \bigcap C| + 1)$$

Proof of the last lemma

Consider $\sum_{v \in V} \sum_{x \in \mathbb{F}} \chi(vx^3)$, and sum it in two ways.

$$q^2 - 2q(\frac{q}{2} - 1) = \sum_{v \in V} \sum_{x \in \mathbb{F}} \chi(vx^3) = \frac{q}{2}(3|V^{\perp} \bigcap C| + 1)$$

$$|V^{\perp} \bigcap C| = 1$$

Proof of the last lemma

Consider $\sum_{v \in V} \sum_{x \in \mathbb{F}} \chi(vx^3)$, and sum it in two ways.

$$q^2 - 2q(\frac{q}{2} - 1) = \sum_{v \in V} \sum_{x \in \mathbb{F}} \chi(vx^3) = \frac{q}{2}(3|V^{\perp} \bigcap C| + 1)$$

$$|V^{\perp} \bigcap C| = 1$$

Proof

Suppose there is a vector space W of dimension m in $\mathrm{NB}_{x^3 + \mathrm{Tr}(x^9)}$.

Proof of the last lemma

Consider $\sum_{v \in V} \sum_{x \in \mathbb{F}} \chi(vx^3)$, and sum it in two ways.

$$q^2 - 2q(\frac{q}{2} - 1) = \sum_{v \in V} \sum_{x \in \mathbb{F}} \chi(vx^3) = \frac{q}{2}(3|V^{\perp} \bigcap C| + 1)$$

$$|V^{\perp} \bigcap C| = 1$$

Proof

Suppose there is a vector space W of dimension m in $\mathrm{NB}_{x^3 + \mathrm{Tr}(x^9)}$.

- $\mathrm{Tr}(w) = 0$ for every $w \in W$. Then $\sum_{x \in \mathbb{F}} \chi(wx^3 + w\mathrm{Tr}(x^9)) = \sum_{x \in \mathbb{F}} \chi(wx^3)$. Using Lemma (Göloğlu and Langevin), we can dismiss this option.

Proof of the last lemma

Consider $\sum_{v\in V}\sum_{x\in\mathbb{F}}\chi(vx^3)$, and sum it in two ways.

$$q^2-2q(\frac{q}{2}-1)=\sum_{v\in V}\sum_{x\in\mathbb{F}}\chi(vx^3)=\frac{q}{2}(3|V^\perp\bigcap C|+1)$$

$$|V^\perp\bigcap C|=1$$

Proof

Suppose there is a vector space W of dimension m in $\mathrm{NB}_{x^3+\mathrm{Tr}(x^9)}$.

- $\mathrm{Tr}(w)=0$ for every $w\in W$. Then $\sum_{x\in\mathbb{F}}\chi(wx^3+w\mathrm{Tr}(x^9))=\sum_{x\in\mathbb{F}}\chi(wx^3)$. Using Lemma (Göloğlu and Langevin), we can dismiss this option.
- $\mathrm{Tr}(w)=0$ for half of the elements of W. Let $V=W\bigcap H_0$, $\alpha\in W:\mathrm{Tr}(\alpha)=1$. Then $\sum_{x\in\mathbb{F}}\chi(wx^3+w\mathrm{Tr}(x^9))=\sum_{x\in\mathbb{F}}\chi(vx^3)+\sum_{x\in\mathbb{F}}\chi((v+\alpha)x^3+x^9)$.

Proof (cont.)

$$\sum_{x \in \mathbb{F}} \chi((v+\alpha)x^3 + x^9) = \begin{cases} 0 \,(\text{impossible (Bracken 2007)}) \\ -2q \\ +2q \end{cases} .$$

Proof (cont.)

$$\sum_{x\in\mathbb{F}} \chi((v+\alpha)x^3 + x^9) = \begin{cases} 0 \,(\text{impossible (Bracken 2007)}) \\ -2q \\ +2q \end{cases}.$$

Consider $\sum_{v\in V}\sum_{x\in\mathbb{F}} \chi((v+\alpha)x^3 + x^9)$.

Proof (cont.)

$$\sum_{x\in\mathbb{F}} \chi((v+\alpha)x^3 + x^9) = \begin{cases} 0 \text{ (impossible (Bracken 2007))} \\ -2q \\ +2q \end{cases}.$$

Consider $\sum_{v\in V}\sum_{x\in\mathbb{F}} \chi((v+\alpha)x^3 + x^9)$.

$$4qM - q^2 = 2qM - 2q(\frac{q}{2} - M) = \sum_{v\in V}\sum_{x\in\mathbb{F}} \chi((v+\alpha)x^3 + x^9) =$$

$$= \sum_{x\in\mathbb{F}} \chi(x^9 + \alpha x^3) \sum_{v\in V} \chi(vx^3) = \frac{q}{2} \pm \frac{3q}{2}$$

Proof (cont.)

$$\sum_{x\in\mathbb{F}} \chi((v+\alpha)x^3 + x^9) = \begin{cases} 0\ (\text{impossible (Bracken 2007)}) \\ -2q \\ +2q \end{cases}.$$

Consider $\sum_{v\in V}\sum_{x\in\mathbb{F}} \chi((v+\alpha)x^3 + x^9)$.

$$4qM - q^2 = 2qM - 2q(\frac{q}{2} - M) = \sum_{v\in V}\sum_{x\in\mathbb{F}} \chi((v+\alpha)x^3 + x^9) =$$

$$= \sum_{x\in\mathbb{F}} \chi(x^9 + \alpha x^3) \sum_{v\in V} \chi(vx^3) = \frac{q}{2} \pm \frac{3q}{2}$$

- $4qM - q^2 = \frac{q}{2} - \frac{3q}{2} = -q$ – cannot happen

Proof (cont.)

$$\sum_{x\in\mathbb{F}} \chi((v+\alpha)x^3 + x^9) = \begin{cases} 0 \,(\text{impossible (Bracken 2007)}) \\ -2q \\ +2q \end{cases} .$$

Consider $\sum_{v\in V}\sum_{x\in\mathbb{F}} \chi((v+\alpha)x^3 + x^9)$.

$$4qM - q^2 = 2qM - 2q(\frac{q}{2} - M) = \sum_{v\in V}\sum_{x\in\mathbb{F}} \chi((v+\alpha)x^3 + x^9) =$$

$$= \sum_{x\in\mathbb{F}} \chi(x^9 + \alpha x^3) \sum_{v\in V} \chi(vx^3) = \frac{q}{2} \pm \frac{3q}{2}$$

- $4qM - q^2 = \frac{q}{2} - \frac{3q}{2} = -q$ – cannot happen
- $4qM - q^2 = \frac{q}{2} + \frac{3q}{2} = 2q$ – also cannot happen

$\square$

Summary

- As of now, no known APN functions are CCZ–equivalent to a permutation in $\mathbb{F}_{2^{12}}$

Summary

- As of now, no known APN functions are CCZ–equivalent to a permutation in $\mathbb{F}_{2^{12}}$
- We have a new EA–invariant for component–wise plateaued functions.

Summary

- As of now, no known APN functions are CCZ–equivalent to a permutation in $\mathbb{F}_{2^{12}}$
- We have a new EA–invariant for component–wise plateaued functions.
- We proven CCZ–inequivalence of $x^3 + \mathrm{Tr}(x^9)$ to a permutation in doubly even extensions.

Thank you for your attention!