Investigating the CCZ-Equivalence between Functions with Low Differential Uniformity by Projected Differential Spectrum

Xi Chen

Co-authors: Longjiang Qu, Chao Li

National University of Defense Technology

July 4, 2017

CONTENT

INTRODUCTION

Introduction

- The design of many block ciphers is based on the classical Shannon idea of the sequential application of confusion and diffusion. Typically, confusion is provided by some form of S-boxes, which are functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$.

- An ideal S-box should have low differential uniformity, high nonlinearity and high algebraic degree etc. Furthermore, for efficient software implementation, S-boxes are often required to be permutations on fields with even degrees.

Introduction

- Finding APN permutations on fields with even degrees is called a BIG open problem.
- Due to the lack of knowledge on APN permutations on $\mathbb{F}_{2^{2k}}$, a natural trade-off solution is to use differentially 4-uniform permutations (4-un.PP for short) as S-boxes.
- For example, AES uses the multiplicative inverse function, which has differential uniformity 4.

Differentially 4-Uniform Permutation

Recently, many new constructions of 4-*un.PP* over $\mathbb{F}_{2^{2k}}$ were constructed by adding a properly chosen Boolean function to the Inverse function. ($G(x) = \frac{1}{x} + f(x)$, 4-uniform BI permutation, $2^{\frac{2^n+2}{3}}$ at least)

Theorem 1.1 (CDZQ16)

Let n be even and f be an n-variable Boolean function. Then $G(x) = \frac{1}{x} + f(\frac{1}{x})$ is a 4-un.PP over $\mathbb{F}_{2^n}$ if and only if $f(x) = f(x+1)$ holds for any $x \in \mathbb{F}_{2^n}$, and for arbitrary $z \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$, at least one of the following two equations holds ($\omega^2 + \omega + 1 = 0$):

$$f(0) + f(z + \frac{1}{z} + 1) + f(\omega z + \frac{1}{\omega z} + 1) + f(\omega^2 z + \frac{1}{\omega^2 z} + 1) = 0,$$

$$f(0) + f(z + \frac{1}{z} + 1) + f(\omega(z + \frac{1}{z} + 1)) + f(\omega^2(z + \frac{1}{z} + 1)) = 1.$$

Differentially 4-Uniform Permutation

Very recently, C.Carlet, D.Tang, X.Tang, et al., presented a new construction of 4-*un.PP* on $\mathbb{F}_{2^{2k}}$, which used the APN property of the inverse function on $\mathbb{F}_{2^{2k-1}}$.
(4-uniform BCTTL permutation, $(2^{n-3} - \lfloor 2^{(n-1)/2-1} \rfloor - 1) \cdot 2^{2^{n-1}}$ at least)

Theorem 1.2 (CTTL14)

Let $n \geq 6$ be even and let $c' \in \mathbb{F}_{2^{n-1}} \setminus \{0, 1\}$ such that $\mathrm{Tr}_1^{n-1}(c') = \mathrm{Tr}_1^{n-1}(\frac{1}{c'}) = 1$, and let f' be an arbitrary Boolean function defined on $\mathbb{F}_{2^{n-1}}$. Then we define an (n, n)-function $F_P(x)$ as follows:

$$F_P(x) = F_P(x_0, x') = \begin{cases} (f'(x'), \frac{1}{x'}), & \text{if } x_0 = 0; \\ (f'(\frac{x'}{c'}) + 1, \frac{c'}{x'}), & \text{if } x_0 = 1, \end{cases}$$

where $x' \in \mathbb{F}_{2^{n-1}}$ is defined as $(x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^{n-1}$. Then $F_P(x)$ is a 4-un pp.

Differentially 4-Uniform Permutation

J.Peng, C.H.Tan, Q.C.Wang, et al. presented a new construction of 4-*un.PP.* (We call them PTW differentially 4-uniform permutations, $2^{\frac{2^{n-1}-2}{3}}$)

Theorem 1.3 (PTW)

Let $n \geq 4$ be an even integer and $S_\alpha = \{\alpha, \frac{\alpha+1}{\alpha}, \frac{1}{\alpha+1}, \alpha+1, \frac{\alpha}{\alpha+1}, \frac{1}{\alpha}\}$, where $\alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$. Assume that $U = \bigcup_{\alpha \in J} S_\alpha$ is the union of some S_α, define an (n, n)-function $G_U(x)$ as

$$G_U(x) = \begin{cases} I(x+1)+1, & \text{if } x \in U; \\ I(x), & \text{if } x \in \mathbb{F}_{2^n} \setminus U, \end{cases}$$

Then $G_U(x)$ is a 4-un.PP.

CCZ-Equivalence

- Two (n, n)-functions are considered to be equivalent if one can be obtained from the other by some simple transformations.
- There are mainly two such equivalence notions, called extended affine equivalence (EA equivalence) and Carlet-Charpin-Zinoviev equivalence (CCZ-equivalence, graph affine equivalence).
- Two equivalent functions have many similar properties.

CCZ-Equivalence

- Proving the CCZ-inequivalence between three functions is mathematically (and also computationally) difficult, unless some CCZ-equivalent invariants can be proved to be different for the two functions.

- Many CCZ-equivalent invariants are known, such as the extended Walsh spectrum, the differential spectra, Γ-rank, Δ-rank, the order of the automorphism group of the design $dev(G_F)$, $dev(D_F)$, etc.

Main problem

- Due to the big cardinality of these two function classes, it seems to be quite difficult to prove or to check the CCZ-equivalence between them even for small fields (grows double exponentially when n grows).
- Moveover, given a 4-*un.PP* on a small field, it also seems difficult to judge whether there exists a function in these three classes which is CCZ-equivalent to the given permutation.

Main idea

- There exist some special R, such that the R-projected differential spectrum of any functions in 4-uniform BI permutation (resp. 4-uniform BCTTL permutation, PTW differentially 4-uniform permutation) are equal.

  Then we may judge the CCZ-equivalent between two classes of functions by calculating only one variant.

- Research the relationship of Projected Differential Spectrum between CCZ-equivalent functions.

PRELIMINARIES

Preliminaries

- Assume $\Gamma(x) \in \mathbb{F}_2[x]$ is an irreducible monic polynomial with degree n and α is a root in the splitting field of $\Gamma(x)$.
  Then $(a_0, a_1, \cdots, a_{n-1})^{\mathsf{T}} \in \mathbb{F}_2^n$ is isomorphic to

$$\mathbb{F}_{2^n} = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \big| a_0, a_1, \cdots, a_{n-1} \in \mathbb{F}_2\}.$$

  In the following, we will switch between these two points of views several times.

Preliminaries

- Differential value: For any $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, let us define the differential value of $F(x)$ at (a, b) as:

$$\delta_F(a, b) = \#\{x \in \mathbb{F}_{2^n} | F(x + a) + F(x) = b\}.$$

Equivalently,

$$\delta_F(a, b) = \# \left\{ (x_1, x_2) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \middle| \begin{bmatrix} \overrightarrow{x_1 + x_2} \\ \overrightarrow{F(x_1) + F(x_2)} \end{bmatrix} = \begin{bmatrix} \vec{a} \\ \vec{b} \end{bmatrix} \right\}.$$

- We remove the usual restriction $a \neq 0$.

Preliminaries

- The multiset $\{* \ \delta_F(a,b) | (a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n} \ *\}$ is called the differential spectrum of F.

- The value

$$\Delta_F := \max_{(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}} \delta_F(a,b)$$

is called the differential uniformity of F.

Preliminaries

- CCZ equivalent: Two functions F and G are called to be Carlet-Charpin-Zinoviev (CCZ) equivalent if there exists an affine permutation $A : \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n}$, such that $A \begin{bmatrix} \vec{y} \\ G(\vec{y}) \end{bmatrix} = \begin{bmatrix} \vec{x} \\ F(\vec{x}) \end{bmatrix}$.
- Let F and G be two CCZ-equivalent (n, n)-functions. We call L a *linearized permutation corresponding to CCZ-equivalent transformation* from G to F if

$$\begin{bmatrix} \vec{x} \\ F(\vec{x}) \end{bmatrix} = L \begin{bmatrix} \vec{y} \\ G(\vec{y}) \end{bmatrix} + \begin{bmatrix} \vec{\xi} \\ \vec{\eta} \end{bmatrix},$$

where $L : \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n}$ is a linearized permutation, and $\vec{\xi}, \vec{\eta}$ are constants on $\mathbb{F}_2^n$.

Preliminaries

- Clearly L^{-1} is also a linearized permutation, and we define the matrix expression of $L^{-1} := \begin{bmatrix} L_1 & L_2 \\ L_3 & L_4 \end{bmatrix}$, where $L_i, i = 1, 2, 3, 4$ are matrixes of $n \times n$ on $\mathbb{F}_2$.
- Let the mapping $\mathcal{L}_i : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, here $\mathcal{L}_i(x)$ is defined by translating its vector expression $\overrightarrow{\mathcal{L}_i(x)} = L_i\vec{x}$ to the finite field.
- Particularly, F and G are extended affine (EA) equivalent when $L_2 = 0$.

PROJECTED DIFFERENTIAL SPECTRUM

Definition of the projected differential spectrum

Definition 3.1

For any $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$*, define the R-projected differential value of F at* (a,b) *as*

$$\delta_{F-R}(a,b) = \sum_{(s,t)\in Ker(R)} \delta_F(a+s, b+t) =$$

$$\sum_{(s,t)\in Ker(R)} \# \left\{ (x_1,x_2) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \middle| \left[\frac{\overrightarrow{x_1 + x_2}}{\overrightarrow{F(x_1)+F(x_2)}} \right] = \left[\frac{\overrightarrow{a+s}}{\overrightarrow{b+t}} \right] \right\}.$$

Furthermore, we define the R-projected differential spectrum of F as the multiset

$$\{* \, \delta_{F-R}(a,b) | (a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \, *\}.$$

Example:

Let $Ker(R) = \{(0,0),(0,1)\}$. Then $\delta_{F-R}(a,b) = \delta_F(a,b) + \delta_F(a,b+1)$.

Relationship between CCZ-equivalent functions

Theorem 3.2

Suppose that two functions F and G are CCZ-equivalent. Let $R : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mapsto \mathbb{F}_2^m$ be a surjective linear function. Let L be a linearized permutation corresponding to CCZ-equivalent transformation from G to F. Then for any $(u, v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, let $\begin{bmatrix} \vec{a} \\ \vec{b} \end{bmatrix} = L \begin{bmatrix} \vec{u} \\ \vec{v} \end{bmatrix}$, we have

$$\delta_{F-R}(a, b) = \delta_{G-R\circ L}(u, v).$$

Proof: According to the definition of CCZ-equivalence, we have

$$\left[\begin{array}{c}\overrightarrow{x_1+x_2}\\ \overrightarrow{F(x_1)+F(x_2)}\end{array}\right]=\left[\begin{array}{c}\vec{x_1}\\ F(\vec{x_1})\end{array}\right]+\left[\begin{array}{c}\vec{x_2}\\ F(\vec{x_2})\end{array}\right]=L\left[\begin{array}{c}\overrightarrow{y_1+y_2}\\ \overrightarrow{G(y_1)+G(y_2)}\end{array}\right].$$

Thus $\left[\begin{array}{c}\overrightarrow{x_1+x_2}\\ \overrightarrow{F(x_1)+F(x_2)}\end{array}\right]=\left[\begin{array}{c}\vec{a}\\ \vec{b}\end{array}\right]\Leftrightarrow\left[\begin{array}{c}\overrightarrow{y_1+y_2}\\ \overrightarrow{G(y_1)+G(y_2)}\end{array}\right]=\left[\begin{array}{c}\vec{u}\\ \vec{v}\end{array}\right]$. Hence

$$\begin{aligned}
&\delta_{F-R}(a,b)\\
=&\sum_{(s_1,t_1)\in Ker(R)}\#\left\{x_1,x_2\in\mathbb{F}_{2^n}\middle|\left[\begin{array}{c}\overrightarrow{x_1+x_2}\\ \overrightarrow{F(x_1)+F(x_2)}\end{array}\right]=\left[\begin{array}{c}\overrightarrow{a+s_1}\\ \overrightarrow{b+t_1}\end{array}\right]\right\}\\
=&\sum_{(s_1,t_1)\in Ker(R)}\#\left\{y_1,y_2\in\mathbb{F}_{2^n}\middle|\left[\begin{array}{c}\overrightarrow{y_1+y_2}\\ \overrightarrow{G(y_1)+G(y_2)}\end{array}\right]=L^{-1}\left[\begin{array}{c}\overrightarrow{a+s_1}\\ \overrightarrow{b+t_1}\end{array}\right]\right\}\\
=&\sum_{(s_2,t_2)\in Ker(R\circ L)}\#\left\{y_1,y_2\in\mathbb{F}_{2^n}\middle|\left[\begin{array}{c}\overrightarrow{y_1+y_2}\\ \overrightarrow{G(y_1)+G(y_2)}\end{array}\right]=\left[\begin{array}{c}\overrightarrow{u+s_2}\\ \overrightarrow{v+t_2}\end{array}\right]\right\}\\
=&\ \delta_{G-R\circ L}(u,v).
\end{aligned}$$

R-projected differential spectrum

R-projected differential spectrum of any 4-uniform BI permutations are equal for some special R.

Property 3.3

4-uniform BI permutation $G(x) = \frac{1}{x} + f(x)$*:*
Let $R : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mapsto \mathbb{F}_2^m$ *be a surjective linear function and* $(0,1) \in Ker(R)$.
Then for any $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, $\delta_{G-R}(a,b) = \delta_{I-R}(a,b)$.

Proof:

$$
\begin{aligned}
& \delta_{G-R}(a,b) \\
= & \#\{x|G(x)+G(x+a)=b+1\}+\#\{x|G(x)+G(x+a)=b\} \\
= & \#\{x|I(x)+I(x+a)+f(x)+f(x+a)=b+1\} \\
& +\#\{x|I(x)+I(x+a)+f(x)+f(x+a)=b\} \\
= & \#\left\{x\middle| \begin{array}{l} I(x)+I(x+a)=b \\ f(x)+f(x+a)=1 \end{array}\right\}+\#\left\{x\middle| \begin{array}{l} I(x)+I(x+a)=b+1 \\ f(x)+f(x+a)=0 \end{array}\right\} \\
& +\#\left\{x\middle| \begin{array}{l} I(x)+I(x+a)=b \\ f(x)+f(x+a)=0 \end{array}\right\}+\#\left\{x\middle| \begin{array}{l} I(x)+I(x+a)=b+1 \\ f(x)+f(x+a)=1 \end{array}\right\} \\
= & \#\left\{x\middle| \begin{array}{l} I(x)+I(x+a)=b+1 \\ f(x)+f(x+a)=1 \end{array}\right\}+\#\left\{x\middle| \begin{array}{l} I(x)+I(x+a)=b+1 \\ f(x)+f(x+a)=0 \end{array}\right\} \\
& +\#\left\{x\middle| \begin{array}{l} I(x)+I(x+a)=b \\ f(x)+f(x+a)=0 \end{array}\right\}+\#\left\{x\middle| \begin{array}{l} I(x)+I(x+a)=b \\ f(x)+f(x+a)=1 \end{array}\right\} \\
= & \#\{x|I(x)+I(x+a)=b+1\}+\#\{x|I(x)+I(x+a)=b\} \\
= & \delta_{I-R}(a,b).
\end{aligned}
$$

R-projected differential spectrum

Property 3.4

4-uniform BCTTL permutation $F_P(x) = F_C(x) + f(x)$:
Let $R : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mapsto \mathbb{F}_2^m$ be a surjective linear function and $(0, 1) \in Ker(R)$. Then for any $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$,

$$\delta_{F_P - R}(a, b) = \delta_{F_C - R}(a, b).$$

Property 3.5

PTW differentially 4-uniform permutation $G_U(x) = \frac{1}{x+f(x)} + f(x)$:
Let $R' : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mapsto \mathbb{F}_2^m$ be a surjective linear function and $(1, 1) \in Ker(R')$. Then for any $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$,

$$\delta_{G_U - R'}(a, b) = \delta_{I - R'}(a, b).$$

APPLICATIONS

Judging CCZ-equivalent by special projections on $\mathbb{F}_2^{2n-1}$

Theorem 4.1

Let $n \geq 6$ be an even integer. Then any function in the form $F_P(x) = F_C(x) + f(x)$ is CCZ-inequivalent to the inverse function $I(x)$, where

$$F_C(x) = F_C(x_0, x') = \begin{cases} (0, \frac{1}{x'}), & \text{if } x_0 = 0; \\ (1, \frac{c'}{x'}), & \text{if } x_0 = 1, \end{cases}$$

Proof: Let $R : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mapsto \mathbb{F}_2^{2n-1}$ be a surjective linear function with $Ker(R) = \{(0,0),(0,1)\}$. According to Theorem 3.2 and Property 3.4, there exists a linearized permutation L corresponding to CCZ-equivalent transformation from I to F_P such that

$$\{* \delta_{F_C - R}(a,b) | (a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} *\} = \{* \delta_{F_P - R}(a,b) | (a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} *\}$$

$$= \{* \delta_{I - R \circ L}(u,v) | (u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} *\}.$$

On one hand, it follows from $Ker(R) = \{(0,0),(0,1)\}$ that for any $a, b \in \mathbb{F}_{2^n}$,

$$\delta_{F_C - R}(a,b) = \delta_{F_C}(a,b) + \delta_{F_C}(a, b+1) \leq 4 \text{ or } 2^n.$$

On the other hand, since $Ker(R \circ L) = \{(0,0), (\mathcal{L}_2(1), \mathcal{L}_4(1))\}$, there exist $u, v \in \mathbb{F}_{2^n}$ such that (proved by Kloosterman Sum)

$$\delta_{I - R \circ L}(u,v) = \delta_I(u,v) + \delta_I(u + \mathcal{L}_2(1), v + \mathcal{L}_4(1)) = 6 \text{ or } 8.$$

Judging CCZ-equivalent by special projections on $\mathbb{F}_2^{2n-2}$

Proposition 4.2

Suppose that $8 \leq n \leq 14$ is an even integer. Then any function in the form $F_P(x) = F_C(x) + f_1(x)$ is CCZ-inequivalent to any function in the form $G(x) = I(x) + f_2(x)$.

Proposition 4.3

Suppose that $6 \leq n \leq 14$ is an even integer. Then any function in the form $F_P(x) = F_C(x) + f_1(x)$ is CCZ-inequivalent to any function in the form $G_U(x)$.

Let $Ker(R) = \{(0,0),(0,1),(s,t),(s,t+1)\}$, where $\begin{bmatrix} \vec{s} \\ \vec{t} \end{bmatrix} = L \begin{bmatrix} \vec{1} \\ \vec{1} \end{bmatrix}$,

Similarly, we can prove Proposition 4.3.

Proof: Let $R : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mapsto \mathbb{F}_2^{2n-2}$ be a surjective linear function satisfying $Ker(R) = \{(0,0),(0,1),(s,t),(s,t+1)\}$, where $\begin{bmatrix} \vec{s} \\ \vec{t} \end{bmatrix} = L \begin{bmatrix} \vec{0} \\ \vec{1} \end{bmatrix}$.

According to Corollary 3.2 and Property 3.4 and Property 3.5, there exists a linearized permutation L corresponding to CCZ-equivalent transformation from $I + f_2$ to $F_C + f_1$ such that

$$\{* \, \delta_{F_C - R}(a,b) | (a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} *\} = \{* \, \delta_{I - R\circ L}(u,v) | (u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} *\}.$$

On one hand, it follows from $Ker(R) = \{(0,0),(0,1),(s,t),(s,t+1)\}$ that for any $a, b \in \mathbb{F}_{2^n}$,

$$\delta_{F_C - R}(a,b) \leq 8 \; or \; \delta_{F_C - R}(a,b) \geq 2^n.$$

On the other hand, since
$Ker(R \circ L) = \{(0,0),(\mathcal{L}_2(1),\mathcal{L}_4(1)),(0,1),(\mathcal{L}_2(1),\mathcal{L}_4(1)+1)\}$.
there exist $u, v \in \mathbb{F}_{2^n}$ such that (verified by Magma)

$$\delta_{I - R\circ L}(u,v) = 10 \; or \; 12.$$

Judging the CCZ-inequivalence on small fields

How to check whether or not there exists any function in the classes of 4-uniform BCTTL permutations, 4-uniform BI permutations or PTW differentially 4-uniform permutations which is CCZ-equivalent to a given 4-un.PP?

- The number of 4-uniform BI permutation on $\mathbb{F}_{2^6}$ is 16198656 ($\approx 2^{23.9}$).
- The number of 4-uniform BCTTL permutation on $\mathbb{F}_{2^6}$ is at least $5 \cdot 2^{32}$.

Judging the CCZ-inequivalence on small fields

For example: Butterfly structure on $\mathbb{F}_{2^6}$

Definition 4.4 (PUB16)

Let T be a bivariate polynomial of $\mathbb{F}_{2^k}$ such that $T_y := x \mapsto T(x, y)$ is a permutation of $\mathbb{F}_{2^k}$ for all y in $\mathbb{F}_{2^k}$. The closed butterfly V_T is the function of $(\mathbb{F}_{2^k})^2$ defined by

$$V_T(x, y) = (T(x, y), T(y, x))$$

and the open butterfly H_T is the permutation of $(\mathbb{F}_{2^k})^2$ defined by

$$H_T(x, y) = (T_{T_y^{-1}(x)}(y), T_y^{-1}(x)),$$

where $T_y(x) = T(x, y)$.

Judging the CCZ-inequivalence on small fields

Theorem 4.5 (PUB16)

Let $k > 1$ be an odd integer and (α, β) be a pair of nonzero elements in $\mathbb{F}_{2^k}$. Assume closed butterfly $V_{T(\alpha,\beta)}$ and open butterfly $H_{T(\alpha,\beta)}$ based on

$$T(x, y) = (x + \alpha y)^3 + \beta y^3.$$

If $\beta \neq (1 + \alpha)^3$, the differential uniformity of $V_{T(\alpha,\beta)}$ and $H_{T(\alpha,\beta)}$ is at most 4. Moreover, it has differential uniformity exactly 4 unless $\beta \in \{(\alpha + \alpha^3), (\alpha^{-1} + \alpha^3)\}$.

Judging the CCZ-inequivalence on small fields

Proposition 4.6

Let $R : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mapsto \mathbb{F}_2^{2n-1}$ *be a surjective linear function satisfying* $Ker(R) = \{(0,0),(0,1)\}$;
Let $R' : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mapsto \mathbb{F}_2^{2n-1}$ *be a surjective linear function satisfying* $Ker(R') = \{(0,0),(1,1)\}$。
If for any $(s,t) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, *multiset*

$$\{* \, \delta_{H_T}(u,v) + \delta_{H_T}(u+s, v+t) | (u,v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \, *\}$$

is not equal to any of these three multisets below, then H_T *is CCZ-inequivalent to any functions in the form above.*
(1) $\{* \, \delta_{I-R}(a,b) | (a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \, *\}$.
(2) $\{* \, \delta_{F_C-R}(a,b) | (a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \, *\}$.
(3) $\{* \, \delta_{I-R'}(a,b) | (a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \, *\}$.

- Notice that

$$\{* \ \delta_{I-R}(a,b) | (a,b) \in \mathbb{F}_{2^6} \times \mathbb{F}_{2^6} \ *\} = \{* 0^{1118} \ 2^{1980} \ 4^{936} \ 6^{60} \ 8^{0} \ 64^{2} *\}.$$

$$\{* \ \delta_{F_C-R}(a,b) | (a,b) \in \mathbb{F}_{2^6} \times \mathbb{F}_{2^6} \ *\} = \{* 0^{k_0} \ 2^{k_2} \ 4^{k_4} \ 6^{0} \ 8^{0} \ (64)^{2} *\}.$$

$$\{* \ \delta_{I-R'}(a,b) | (a,b) \in \mathbb{F}_{2^6} \times \mathbb{F}_{2^6} \ *\} = \{* 0^{1152} \ 2^{1980} \ 4^{840} \ 6^{120} \ 8^{2} \ 68^{2} *\}.$$

  It can be verified by Magma that for any $s, t \in \mathbb{F}_{2^6}$, the projected differential spectrum

$$\{* \ \delta_{H_T}(u,v) + \delta_{H_T}(u+s, v+t) | (u,v) \in \mathbb{F}_{2^6} \times \mathbb{F}_{2^6} \ *\}$$

  is not equal to any multiset above.
  Thus it is CCZ-inequivalence to any functions in the three great classes of 4-un.PPs.
- One can check it is CCZ-inequivalence to any other known 4-un.PPs by CCZ-equivalent invariants.

THANK YOU !