On Sboxes sharing the same DDT

Christina Boura, Anne Canteaut, Jérémy Jean, Valentin Suder

BFA, Loen, Norway,

June 18, 2018

Problem

Find all n-bit Sboxes having a given difference distribution table (DDT).

α/β	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

where $\delta_F(\alpha, \beta) = \#\{x \in \mathbb{F}_2^n : F(x + \alpha) + F(x) = \beta\}$

Some trivial properties of the DDT

Differential uniformity of F [Nyberg 93]:

$$\delta(F) = \max_{\alpha \neq 0, \beta} \delta_F(\alpha, \beta)$$

$\delta(F) \geq 2$ with equality for APN functions.

- All entries in the DDT are even.
- The entries in a row sum to 2^n.

Related open problems

- Characterization of valid DDTs.
- Characterization of the functions sharing the same DDT.
- **The big APN problem** [Dillon 09]: Does there exist an APN permutation of n variables with n even, $n \geq 8$?
- **The crooked conjecture** [Bending, Fon-der-Flaass 98]: F is an APN permutation of degree 2 if and only if the support of every row in the DDT is the complement of a hyperplane.

Indicator of the DDT [Carlet, Charpin, Zinoviev 98]

Definition: For any n-bit Sbox F, γ_F is the Boolean function of $2n$ variables defined by

$$\gamma_F(\alpha, \beta) = 0 \text{ if and only if } \delta_F(\alpha, \beta) = 0 \text{ or } \alpha = 0.$$

Example:

α/β	0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0	2	0	2	0	2	0	2
2	0	0	2	2	0	0	2	2
3	0	2	2	0	0	2	2	0
4	0	0	0	0	2	2	2	2
5	0	2	0	2	2	0	2	0
6	0	0	2	2	2	2	0	0
7	0	2	2	0	2	0	0	2

Indicator of the DDT [Carlet, Charpin, Zinoviev 98]

Definition: For any n-bit Sbox F, γ_F is the Boolean function of $2n$ variables defined by

$$\gamma_F(\alpha, \beta) = 0 \text{ if and only if } \delta_F(\alpha, \beta) = 0 \text{ or } \alpha = 0.$$

Example:

α/β	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	*	*	*	**0**	*	0	*
2	0	0	*	*	0	0	*	*
3	0	*	*	0	0	*	*	0
4	0	0	0	0	*	*	*	*
5	0	*	0	*	*	0	*	0
6	0	0	*	*	*	*	0	0
7	0	*	*	0	*	0	0	*

- $\gamma(1, 1) = 1$
- $\gamma(1, 4) = 0$

Two notions of differential equivalence

- DDT-equivalence:

$$F \sim_{\mathrm{DDT}} G \quad \Leftrightarrow \quad \mathrm{DDT}_F = \mathrm{DDT}_G$$

- γ-equivalence (aka differential equivalence [Gorodilova 16]):

$$F \sim_{\gamma} G \quad \Leftrightarrow \quad \gamma_F = \gamma_G$$

Remark:

DDT-equivalence $\Rightarrow$ γ-equivalence

The two notions are different

Example $(n = 4)$

$$F = [\texttt{0,1,2,3,4,5,6,7,8,9,10,11,12,13,15,14}]$$

$$G = [\texttt{0,1,3,2,5,4,7,6,8,9,10,11,12,13,14,15}]$$

$$\mathrm{DDT}_F = \begin{bmatrix}
16 & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & 16 & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & 12 & 4 & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & 4 & 12 & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & 12 & 4 & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & 4 & 12 & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & 12 & 4 & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & 4 & 12 & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & 12 & 4 & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & 4 & 12 & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & 12 & 4 & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & 4 & 12 & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & 12 & 4 & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & 4 & 12 & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & 12 & 4 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & 4 & 12
\end{bmatrix}$$

The two notions are different

Example $(n = 4)$

$$F = [\texttt{0,1,2,3,4,5,6,7,8,9,10,11,12,13,15,14}]$$
$$G = [\texttt{0,1,3,2,5,4,7,6,8,9,10,11,12,13,14,15}]$$

$$\mathrm{DDT}_G = \begin{bmatrix}
16 & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & 16 & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & 12 & 4 & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & 4 & 12 & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & 12 & 4 & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & 4 & 12 & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & 12 & 4 & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & 4 & 12 & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & 4 & 12 & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & 12 & 4 & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & 4 & 12 & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & 12 & 4 & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & 4 & 12 & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & 12 & 4 & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & 4 & 12 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & 12 & 4
\end{bmatrix}$$

γ-equivalence and differential uniformity

Obviously, two DDT-equivalent functions F and G have the same differential uniformity.

However, two γ-equivalent functions **do not** necessary have the same differential uniformity.

The following 4-bit Sboxes are γ-equivalent.

$$F_1 = [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0] \text{ with } \delta(F_1) = 14$$

$$F_2 = [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1] \text{ with } \delta(F_2) = 12$$

$$F_3 = [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1] \text{ with } \delta(F_3) = 10$$

$$F_4 = [1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1] \text{ with } \delta(F_4) = 8$$

α/β	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
1	14	2	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	14	2	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	14	2	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	14	2	.	.	.	.	.	.	.	.	.	.	.	.	.	.
5	14	2	.	.	.	.	.	.	.	.	.	.	.	.	.	.
6	14	2	.	.	.	.	.	.	.	.	.	.	.	.	.	.
7	14	2	.	.	.	.	.	.	.	.	.	.	.	.	.	.
8	14	2	.	.	.	.	.	.	.	.	.	.	.	.	.	.
9	14	2	.	.	.	.	.	.	.	.	.	.	.	.	.	.
10	14	2	.	.	.	.	.	.	.	.	.	.	.	.	.	.
11	14	2	.	.	.	.	.	.	.	.	.	.	.	.	.	.
12	14	2	.	.	.	.	.	.	.	.	.	.	.	.	.	.
13	14	2	.	.	.	.	.	.	.	.	.	.	.	.	.	.
14	14	2	.	.	.	.	.	.	.	.	.	.	.	.	.	.
15	14	2	.	.	.	.	.	.	.	.	.	.	.	.	.	.

$$F_1 = [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0] \text{ with } \delta(F_1) = 14$$

α/β	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
1	12	4	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	12	4	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	12	4	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
5	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
6	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
7	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
8	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
9	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
10	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
11	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
12	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
13	12	4	.	.	.	.	.	.	.	.	.	.	.	.	.	.
14	12	4	.	.	.	.	.	.	.	.	.	.	.	.	.	.
15	12	4	.	.	.	.	.	.	.	.	.	.	.	.	.	.

$F_2 = [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1]$ with $\delta(F_2) = 12$

α/β	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
1	10	6	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	10	6	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	10	6	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	10	6	.	.	.	.	.	.	.	.	.	.	.	.	.	.
5	10	6	.	.	.	.	.	.	.	.	.	.	.	.	.	.
6	10	6	.	.	.	.	.	.	.	.	.	.	.	.	.	.
7	6	10	.	.	.	.	.	.	.	.	.	.	.	.	.	.
8	6	10	.	.	.	.	.	.	.	.	.	.	.	.	.	.
9	6	10	.	.	.	.	.	.	.	.	.	.	.	.	.	.
10	6	10	.	.	.	.	.	.	.	.	.	.	.	.	.	.
11	10	6	.	.	.	.	.	.	.	.	.	.	.	.	.	.
12	6	10	.	.	.	.	.	.	.	.	.	.	.	.	.	.
13	10	6	.	.	.	.	.	.	.	.	.	.	.	.	.	.
14	10	6	.	.	.	.	.	.	.	.	.	.	.	.	.	.
15	10	6	.	.	.	.	.	.	.	.	.	.	.	.	.	.

$F_3 = [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1]$ with $\delta(F_3) = 10$

α/β	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
1	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
5	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
6	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
7	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
8	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
9	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
10	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
11	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
12	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
13	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
14	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.
15	8	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.

$F_4 = [1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1]$ with $\delta(F_4) = 8$

The two notions coincide in some cases

Proposition. Suppose that $F \sim_\gamma G$. If each derivative of F and G is λ-to-1 for some λ, then $F \sim_{\mathrm{DDT}} G$.

α/β	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	2	.	.	.	2	2
2	.	2	2	.	.	.	2	2
3	.	4	.	.	.	4	.	.
3	.	.	.	.	4	4	.	.
5	.	2	2	.	.	.	2	2
6	.	2	2	.	.	.	2	2
7	.	4	.	.	4	.	.	.

Notably, this result holds when

- F is APN.
- F and G are quadratic.

Outline

1. Sboxes sharing the same DDT

2. Experimental Results

Trivially equivalent Sboxes

Proposition. The DDT-equivalence class of $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ contains all functions of the form

$$x \mapsto F(x + c) + d, \text{ for } c, d \in \mathbb{F}_2^n.$$

- The DDT-equivalence class of F is trivial if it contains trivially equivalent Sboxes only.

Problems

- Characterize the Sboxes having a trivial DDT-equivalence class.
- Determine the properties of the Sboxes within a non-trivial DDT-equivalence class.

An equivalent formulation

F and G share the same DDT iff they share the same squared LAT.

$\Rightarrow$ Sboxes within the same DDT-equivalence class correspond to LAT with different sign sequences:

$$\mathcal{W}_G(\lambda, \mu) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\lambda \cdot G(x) + \mu \cdot x} = (-1)^{s(\lambda,\mu)} \mathcal{W}_F(\lambda, \mu).$$

F and $G = F(x + c) + d$ are trivially DDT-equivalent Sboxes if and only if

$$s(\lambda, \mu) = d \cdot \lambda + c \cdot \mu.$$

Algebraic degree of DDT-equivalent Sboxes

Conjecture [Gorodilova 16]. If F is a quadratic APN Sbox, then any G in the DDT-class of F satisfies

$$\deg(F+G) \leq 1.$$

In general: For any even n, all n-bit Sboxes defined by

$$S(x) = (f(x), c_1, \ldots, c_{n-1})$$

where f is a bent function and $(c_1, \ldots, c_{n-1})$ is a constant, have the same DDT. All rows are equal to

$$[2^{n-1}, 2^{n-1}, 0, 0, \ldots, 0]$$

$\Rightarrow$ There exist Sboxes of any degree between $\mathbf{2}$ and $\boldsymbol{n/2}$ in this DDT-equivalence class.

An example

$$F = [1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1] \text{ with } \deg(F) = 2.$$

- The DDT-equivalence class of F contains $7168 = (28 \times 2^5) \times 2^3$ functions.
- $F' = [1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1]$ is non-trivially DDT-equivalent to F and $\deg(F') = 2$.

But,

$$\deg(F + F') = 2.$$

Extended-affine equivalence

Two functions $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are extended-affine (EA) equivalent if there exist affine functions A_0, A_1, A_2, where A_1 and A_2 are bijective such that

$$G = A_1 \circ F \circ A_2 + A_0.$$

Proposition (adapted from [Gorodilova 16])
If F and G are EA-equivalent then their DDT and γ-equivalence classes **have the same size**.

Moreover,

$$\mathcal{C}_{\mathrm{DDT}}(G) = \{A_1 \circ F' \circ A_2 + A_0, \text{ with } F' \in \mathcal{C}_{\mathrm{DDT}}(F)\}$$

CCZ equivalence [Carlet, Charpin, Zinoviev 98]

Two functions $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are said CCZ equivalent if

$$\{(x, G(x)), x \in \mathbb{F}_2^n\} \text{ is the image of } \{(x, F(x)), x \in \mathbb{F}_2^n\}$$

by a linear permutation $\mathcal{L}$ of $\mathbb{F}_2^n \times \mathbb{F}_2^n$.

In particular, if

$$\mathcal{L} : (x, y) \mapsto (L_1(x, y), L_2(x, y)),$$

then $x \mapsto L_1(x, F(x))$ is a permutation.

Open problem [Gorodilova '16]

Does an analogue of the result for EA equivalence hold for CCZ equivalence ?

CCZ equivalence

Theorem. If F and G are CCZ-equivalent then

- their DDT (resp. γ-equivalence) classes have the same size.
- The DDT-class of G is obtained by applying the same linear permutation $\mathcal{L}$ to all functions in the DDT-class of F.

Algorithm for computing the DDT and γ-equivalence classes

Input : a DDT (resp. indicator or a DDT),
Output : **All functions** having this DDT (resp. indicator)

Idea: Recursive Tree-traversal algorithm

- Tree of depth 2^n : each node at level i corresponds to one **possible value** for $F(i)$.
- From the constraints of the DDT and the values $F(0), \ldots, F(i-1)$:
  - find **all possible values** for $F(i)$
  - **for each** of them, move on to the next step $F(i+1)$, and **backtrack** if necessary

Pruning trick: Fix $F(0)$

Example for $n = 3$

$$\mathcal{R}_i := \{j \mid \mathrm{DDT}(i,j) \neq 0\}. \quad \textbf{Ex.} \ \mathcal{R}_1 = \{1,3,5,7\}$$

	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$

Example for $n = 3$

$$\mathcal{R}_i := \{j \mid \mathrm{DDT}(i,j) \neq 0\}. \quad \textbf{Ex.} \ \ \mathcal{R}_1 = \{1,3,5,7\}$$

	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$
1. $F(0) + F(1) \in \mathcal{R}_1 = \{1,3,5,7\}$
   Set $F(1) = 1$

Example for $n = 3$

$$\mathcal{R}_i := \{j \mid \mathrm{DDT}(i,j) \neq 0\}. \quad \textbf{Ex.} \;\; \mathcal{R}_1 = \{1,3,5,7\}$$

	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$
1. $F(0) + F(1) \in \mathcal{R}_1 = \{1,3,5,7\}$
   Set $F(1) = 1$
2. $F(0) + F(2) \in \mathcal{R}_2 = \{2,3,6,7\}$

Example for $n = 3$

$$\mathcal{R}_i := \{j \mid \mathrm{DDT}(i,j) \neq 0\}. \quad \textbf{Ex.} \;\; \mathcal{R}_1 = \{1,3,5,7\}$$

	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$
1. $F(0) + F(1) \in \mathcal{R}_1 = \{1,3,5,7\}$
   Set $F(1) = 1$
2. $F(0) + F(2) \in \mathcal{R}_2 = \{2,3,6,7\}$ and
   $F(1) + F(2) \in \mathcal{R}_3 = \{1,2,5,6\}$

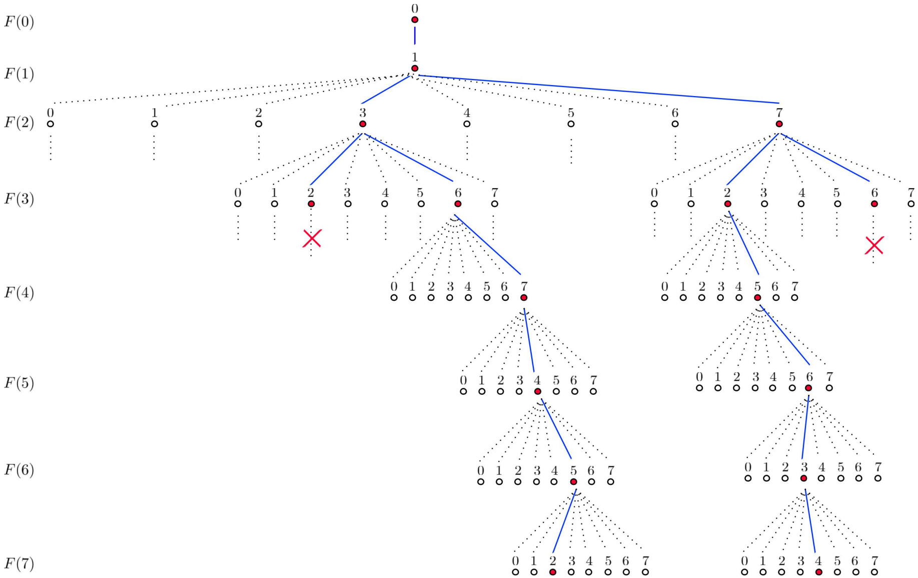
Example for $n = 3$

$$\mathcal{R}_i := \{j \mid \mathrm{DDT}(i,j) \neq 0\}. \quad \textbf{Ex.} \;\; \mathcal{R}_1 = \{1,3,5,7\}$$

	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$
1. $F(0) + F(1) \in \mathcal{R}_1 = \{1,3,5,7\}$
   Set $F(1) = 1$
2. $F(0) + F(2) \in \mathcal{R}_2 = \{2,3,6,7\}$ and
   $F(1) + F(2) \in \mathcal{R}_3 = \{1,2,5,6\}$ thus

   $F(2) \in F(0) + \mathcal{R}_2 \cap F(1) + \mathcal{R}_3 = \{3,7\}$


$F(0)$
$F(1)$
$F(2)$
$F(3)$
$F(4)$
$F(5)$
$F(6)$
$F(7)$
0
1
0 1 2 3 4 5 6 7
0 1 2 3 4 5 6 7
0 1 2 3 4 5 6 7
0 1 2 3 4 5 6 7
0 1 2 3 4 5 6 7
0 1 2 3 4 5 6 7
0 1 2 3 4 5 6 7
0 1 2 3 4 5 6 7
0 1 2 3 4 5 6 7
0 1 2 3 4 5 6 7
0 1 2 3 4 5 6 7

Outline

Permutations with optimal differential uniformity

APN permutations

The DDT-equivalence classes of all known APN permutations for $n \leq 9$ are trivial.

Optimal permutations for $n = 4$

The DDT-equivalence classes and the γ-equivalence classes of all permutations F with $\delta(F) = 4$ and optimal linearity listed in [Leander, Poschmann 07] are trivial.

APN non-bijective functions

The DDT-equivalence classes of all known APN functions for $n \leq 8$ are trivial, except:

- when $n \equiv 0 \mod 4$: the Gold APN functions with exponents $2^k + 1$ with $k = n/2 \pm 1$ [Gorodilova 16]
- for $n = 6$: Class 13 in [Brinckmann, Leander 08].

We checked that, for $n = 6$, all APN functions of degree ≤ 3 are trivial except Class 13.

Do all permutations have a trivial DDT class?

The following permutations share the same DDT.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$F(x)$	0	1	2	3	4	5	6	7	8	9	10	11	13	12	15	14	16
$G(x)$	0	1	2	3	4	5	6	7	8	9	10	11	13	12	15	14	16

x	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$F(x)$	17	19	18	20	21	23	22	25	24	26	27	28	29	31	30
$G(x)$	17	19	18	21	20	22	23	24	25	27	26	28	29	31	30

However, F and G are not trivially equivalent.

Some conclusions and a conjecture

- All Sboxes we found with a non-trivial DDT-equivalence class have non-distinct rows in their DTT.
- All rows in the DDT of an APN permutation are distinct.

Conjecture.
The DDT-equivalence class of any APN permutation is trivial.

Open problem.
Find a family of Sboxes for which it can be proved that the DDT-equivalence class is trivial.