On Sboxes sharing the same DDT

Christina Boura, Anne Canteaut, Jérémy Jean, Valentin Suder

To cite this version:

Christina Boura, Anne Canteaut, Jérémy Jean, Valentin Suder. On Sboxes sharing the same DDT. Dagstuhl Seminar 18021 Symmetric Cryptography, Jan 2018, Dagstuhl, Germany. 10.4230/DAGREP.8.1.1 . hal-01955256

HAL Id: hal-01955256
https://hal.inria.fr/hal-01955256

Submitted on 14 Dec 2018

On Sboxes sharing the same DDT

Christina Boura, Anne Canteaut, Jérémy Jean, Valentin Suder

University of Versailles, France
Inria Paris, France
Anssi, France

Dagstuhl seminar, January 11, 2018

Problem

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

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:

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

$\delta(F) \geq 2$ 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

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

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

Two notions of differential equivalence

- DDT-equivalence:

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

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

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

DDT-equivalence $\Rightarrow$ γ-equivalence

The two notions are different

For $n = 4$

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

G = [0,1,3,2,5,4,7,6,8,9,10,11,12,13,14,15].

$$\mathbf{DDT}_{F} = \begin{bmatrix}
\mathbf{16} & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & \mathbf{16} & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & \mathbf{12} & \mathbf{4} & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & \mathbf{4} & \mathbf{12} & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & \mathbf{12} & \mathbf{4} & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & \mathbf{4} & \mathbf{12} & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & \mathbf{12} & \mathbf{4} & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & \mathbf{4} & \mathbf{12} & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & \mathbf{12} & \mathbf{4} & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & \mathbf{4} & \mathbf{12} & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & \mathbf{12} & \mathbf{4} & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & \mathbf{4} & \mathbf{12} & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & \mathbf{12} & \mathbf{4} & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & \mathbf{4} & \mathbf{12} & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & \mathbf{12} & \mathbf{4} \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & \mathbf{4} & \mathbf{12}
\end{bmatrix}$$

The two notions are different

For $n = 4$

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

$G =$ `[0,1,3,2,5,4,7,6,8,9,10,11,12,13,14,15]`.

$$\mathbf{DDT}_G = \begin{bmatrix}
16 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & 16 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & 12 & 4 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & 4 & 12 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & 12 & 4 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & 4 & 12 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 12 & 4 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 4 & 12 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 4 & 12 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 12 & 4 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 4 & 12 & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 12 & 4 & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 4 & 12 & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 12 & 4 & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 4 & 12 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 12 & 4
\end{bmatrix}$$

γ-equivalence and differential uniformity

The following 4-bit Sboxes are γ-equivalent:

$\boldsymbol{F_1} =$ `[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]` with $\boldsymbol{\delta(F_1) = 14}$,
$\boldsymbol{F_2} =$ `[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1]` with $\boldsymbol{\delta(F_2) = 12}$,
$\boldsymbol{F_3} =$ `[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1]` with $\boldsymbol{\delta(F_3) = 10}$,
$\boldsymbol{F_4} =$ `[1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1]` with $\boldsymbol{\delta(F_4) = 8}$.

The two notions coincide in some cases

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

$F \sim_\gamma G$ implies $F \sim_{\textsf{DDT}} G$

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

Sboxes sharing the same DDT

Trivially equivalent Sboxes

Proposition.

The DDT-equivalence class of an n-bit Sbox contains all functions of the form

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

We say that 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

$\boldsymbol{F}$ and $\boldsymbol{G}$ 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:

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

$\boldsymbol{F}$ and $\boldsymbol{G}$ are trivially DDT-equivalent Sboxes if and only if

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

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 2 and $n/2$ in this DDT-equivalence class.

Extended affine equivalence

Definition.

Two n-bit Sboxes F and G 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-equivalence (resp. γ-equivalence) classes have the same size.

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

CCZ equivalence [Carlet, Charpin, Zinoviev 98]

Definition.

Two n-bit Sboxes F and G are said CCZ equivalent if

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

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

$$x \mapsto L_1(x, F(x)) \text{ is a permutation.}$$

Open problem [Gorodilova 16]

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

CCZ equivalence

Theorem.
If $\boldsymbol{F}$ and $\boldsymbol{G}$ are CCZ-equivalent then

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

Algorithm for determining all Sboxes having a prescribed γ

Input : The indicator of a DDT,
Output : All functions having this indicator

Idea: Recursive Tree-traversal algorithm

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

Pruning trick: We fix

$$\boldsymbol{F}(0) \text{ and } \boldsymbol{F}(1)$$

Experimental results

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 $n \equiv 0 \bmod 4$: 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

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.

Toy example for $n = 3$

$$\mathcal{R}_i := \{j \mid \mathsf{DDT}(i,j) \neq 0\}.$$

	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

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

Toy example for $n = 3$