Two Notions of Differential Equivalence on Sboxes

Christina Boura, Anne Canteaut, Jérémy Jean, Valentin Suder

To cite this version:

Christina Boura, Anne Canteaut, Jérémy Jean, Valentin Suder. Two Notions of Differential Equivalence on Sboxes. Designs, Codes and Cryptography, In press, 87 (2-3), pp.185-202. 10.1007/s10623-018-0496-z . hal-01944565

HAL Id: hal-01944565

https://inria.hal.science/hal-01944565

Submitted on 4 Dec 2018

Two Notions of Differential Equivalence on Sboxes

Christina Boura[1,2], Anne Canteaut[2], Jérémy Jean[3], and Valentin Suder[1]

[1] University of Versailles, France
Christina.Boura@uvsq.fr, Valentin.Suder@uvsq.fr

[2] Inria, France
Anne.Canteaut@inria.fr

[3] ANSSI, France
Jeremy.Jean@ssi.gouv.fr

Abstract. In this work, we discuss two notions of differential equivalence on Sboxes. First, we introduce the notion of *DDT-equivalence* which applies to vectorial Boolean functions that share the same difference distribution table (DDT). Next, we compare this notion to what we call the γ*-equivalence*, applying to vectorial Boolean functions whose DDTs have the same support. We discuss the relation between these two equivalence notions, demonstrate that the number of DDT- or γ-equivalent functions is invariant under EA- and CCZ-equivalence and provide an algorithm for computing the DDT-equivalence and the γ-equivalence classes of a given function. We study the sizes of these classes for some families of Sboxes. Finally, we prove a result that shows that the rows of the DDT of an APN permutation are pairwise distinct.

Keywords. Boolean function, Sbox, APN, difference distribution table, equivalence.

1 Introduction

Block ciphers are central primitives in symmetric encryption schemes. Modern block ciphers are designed based on a methodology which guarantees that the cipher is resistant against all classical attacks. Differential cryptanalysis, presented by Biham and Shamir in 1990 [BS91], is one of the most prominent attacks against block ciphers, and a precise evaluation of its complexity has led to some design criteria on the building blocks in the cipher. The main criterion, which has been introduced by Nyberg and Knudsen [NK93, Nyb94], is the so-called differential uniformity of the Sbox, i.e., of the nonlinear mapping used in the cipher. This parameter should be as small as possible in order to maximize the complexity of differential attacks, and the mappings with the lowest differential uniformity, named APN mappings, have been investigated in many works during the last twenty-five years. These mappings are indeed highly relevant for cryptographic applications and they are also optimal combinatorial objects of independent interest. Therefore, this design criterion is at the origin of a whole line of research, including the search for infinite families of permutations with a low differential uniformity, the study of their properties or some classification work (e.g. [Nyb94, CV95, CCZ98, Dob99, BDMW10, HM11, EKP06]).

However, besides the differential uniformity of the Sbox, the whole differential spectrum and even the form of the difference distribution table (DDT) are important when the resistance against several variants of differential cryptanalysis is quantified. The number of occurrences of the differential uniformity in the DDT of the Sbox corresponds to the number of one-round differentials with the highest probability and should then be minimized. Also, the whole differential spectrum of the Sbox is involved in all known upper-bounds on the maximal expected differential probability over two rounds of an SPN cipher [PSLL03, CR15]. Not only the number, but also the location within the DDT of these maximal values may influence the resistance of the cipher against multiple differential cryptanalysis [BG11] or truncated differential attacks [Knu95] (see e.g. [BCC10, Section 3.2] for a discussion). When designing a block cipher, it would then be of major interest to be able to start from a desired DDT which guarantees a high resistance against all variants of differential cryptanalysis, and to construct Sboxes having this specific DDT. Instead, the main technique currently available to the designers consists in randomly generating Sboxes until one with a suitable DDT is found. However, constructing Sboxes from a prescribed DDT is a difficult problem, related to many open issues in the area. The characterization of the valid DDT, i.e., for which there exists at least one function with these particular DDT, is also open. In the case of APN functions, this general problem corresponds to the problem of determining the *differential equivalence class* of a given function, introduced by Gorodilova [Gor16]. It has also been raised by Carlet in the case of APN functions [Car15, Pb. 3.11]. It is obviously related to the so-called *Big APN problem*, i.e., the existence of APN permutations operating on an even number of variables. Indeed, it has been long conjectured that bijective APN functions do only exist in odd dimension, until the first ever counter-example over $\mathbb{F}_2^6$ was presented by Dillon et al. [BDMW10]. However, the conjecture still stands for any even dimension $n \geq 8$.

Our Contributions. In this work, we are interested in two different equivalence notions for vectorial Boolean functions, that we call DDT and γ-equivalence. The first one applies to functions sharing the same difference distribution table while the second, applies more generally to functions whose DDT have the same support. In [Gor16], Gorodilova studies the γ-equivalence classes for quadratic APN functions and in particular for the Gold family of functions. She most notably proves that the size of the γ-classes for any function is invariant under extended affine (AE) equivalence. Gorodilova wonders then whether something similar can be proved for CCZ-equivalence. In this work, we give an answer to this question by proving that the number of elements in the differential class of a function is invariant under CCZ-equivalence.

In parallel, we also provide an algorithm for computing the differential equivalence class corresponding to a prescribed DDT. We applied this algorithm to find several equivalence classes. Most notably, one of the main problems we focus on is to determine whether the differential equivalence class of a *permutation* over $\mathbb{F}_2^n$ can contain more than 2^{2n} elements. In other words, we wonder whether two permutations F and G with the same DDT necessarily satisfy $G(x) = F(x \oplus c) \oplus d$ for some $c, d \in \mathbb{F}_2^n$. As a result, we found permutations F whose differential equivalence classes contain other elements than the functions $x \mapsto F(x \oplus c) \oplus d$. However, we conjecture that this is only the case when some rows of the corresponding DDT are equal. We also discuss some properties of the DDT of an APN permutation, adding some constraints on the valid DDT for such permutations.

2 Two Notions of Differential Equivalence

Even if the following properties hold in the general case, our work mainly focuses on vectorial Boolean functions with the same number of inputs and outputs, i.e., on functions from $\mathbb{F}_2^n$ into itself. Several cryptographic Sboxes are examples of such functions, which usually verify additional properties for cryptographic applications, most notably nonlinearity. Although we focus on Sboxes in the remainder of this paper, most of the results can be adapted to general vectorial Boolean functions.

2.1 DDT-equivalence and γ-equivalence

The differential properties of a vectorial Boolean function are related to its derivatives.

Definition 1 (Derivative of a function). *Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$. The* derivative of F with respect to $a \in \mathbb{F}_2^n$ *is the function*

$$\Delta_a F : x \in \mathbb{F}_2^n \mapsto F(x \oplus a) \oplus F(x).$$

The constant derivatives of a function often play a major role and correspond to its *linear structures.*

Definition 2 (Linear space and linear structures of a function). *Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$. An element $a \in \mathbb{F}_2^n$ is called a* linear structure *of F if $\Delta_a F$ is constant. The set of all linear structures is a vector space named* the linear space *of F.*

The multi-sets corresponding to the images of the derivatives of F are usually represented as a two-dimensional array called the difference distribution table.

Definition 3 (DDT and its characteristics). *Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$. The* difference distribution table (DDT) *of F is the two-dimensional table defined by*

$$\delta_F(a,b) = \#\{x \in \mathbb{F}_2^n : \Delta_a F(x) = b\}, \;\; \forall a,b \in \mathbb{F}_2^n.$$

Two important characteristics of the DDT, introduced in [Nyb94, CCZ98] respectively, are as follows:

- *the* differential uniformity of F *is the highest value in the DDT, i.e.*

  $$\max_{a,b \in \mathbb{F}_2^n, a\neq 0} \delta_F(a,b).$$

  The lowest possible value for the differential uniformity of a function from $\mathbb{F}_2^n$ into itself is two and the functions with differential uniformity two are called almost perfect nonlinear (APN)*.*
- *the* indicator of the DDT *is the Boolean function of $2n$ variables defined by*

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

The previous properties then lead to two different notions of equivalence between Sboxes. We say that F and G are DDT-equivalent if they have the same DDT, and that they are γ-equivalent if their DDTs have the same support, or equivalently if $\gamma_F = \gamma_G$.

The notion of γ-equivalence has been investigated under the name *differential equivalence* by Gorodilova [Gor16]. It must not be confused with the *differential equivalence* introduced in [Sud15, Sud17], which refers to another property.

Obviously, DDT-equivalence implies γ-equivalence. However, the converse also holds in some particular cases.

Proposition 1. *Let F and G be two functions from $\mathbb{F}_2^n$ into itself which are γ-equivalent. Assume that, for each derivative of F and G, there exists some integer λ such that the derivative is a λ-to-1 function. Then, F and G are DDT-equivalent. Most notably, this situation holds when both F and G are quadratic functions. It also implies that any function which is γ-equivalent to an APN function F is also DDT-equivalent to F.*

Proof. The result comes from the fact that, in this case, the DDT of the function is entirely determined by its support. Assume that, for any $a \in \mathbb{F}_2^n$, $a \neq 0$, $\Delta_a F$ is a λ-to-1 function (where λ may depend on a). Then, the entries of the row in the DDT corresponding to $\Delta_a F$ belong to $\{0, \lambda\}$. Since the sum of all entries within a row equals 2^n, we deduce that λ is a power of two, and its value can be deduced from the number of elements b such that $\gamma_F(a,b) = 1$ which equals $2^n\lambda^{-1}$. Then, the row corresponding to $\Delta_a F$ is entirely deduced from γ_F. When F is a quadratic function, its derivatives have degree at most one. Then, $\Delta_a F$ is a 2^d-to-1 function where d is the dimension of the kernel of $\Delta_a F$. □

It is worth noticing that the previous proposition does not mean that the γ-equivalence class of a quadratic function equals its DDT-equivalence class. A quadratic function F such that $\mathcal{C}_\gamma(F) \neq \mathcal{C}_{\mathsf{DDT}}(F)$ is exhibited at the end of Section 2.2. However, the two notions coincide for APN functions, for instance for the quadratic APN functions studied in [Gor16] and in [YWL14], implying that the γ-equivalent APN functions exhibited in [Gor16] are also DDT-equivalent.

In general, the two notions of differential equivalence do not coincide. The following example exhibits two γ-equivalent functions with different DDTs.

Example 1. Let F and $G : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ be represented by their value tables:

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

Both DDTs are diagonal with 2×2 blocks, the first block being $\begin{bmatrix} 16 & 0 \\ 0 & 16 \end{bmatrix}$ for both tables. Then, for F, all the diagonal blocks are $\begin{bmatrix} 12 & 4 \\ 4 & 12 \end{bmatrix}$, whereas for G, half of the blocks only are of this shape, the other ones are $\begin{bmatrix} 4 & 12 \\ 12 & 4 \end{bmatrix}$. It is then clear that F and G, who are both of algebraic degree three, are γ-equivalent, but are not DDT-inequivalent.

2.2 Properties of differential-equivalence classes

In this work, we mainly focus on the sizes of the DDT-equivalence classes and γ-equivalence classes. A lower bound on these sizes is given in the following proposition.

Proposition 2. *Let F be a function from $\mathbb{F}_2^n$ into itself and let ℓ denote the dimension of its linear space, i.e., of the space formed by all linear structures of F. Then, the DDT-equivalence class of F contains the $2^{2n-\ell}$ distinct functions of the form*

$$x \mapsto F(x \oplus c) \oplus d, \quad c, d \in \mathbb{F}_2^n. \tag{1}$$

Proof. The fact that all functions $F_{c,d} : x \mapsto F(x \oplus c) \oplus d$ are DDT-equivalent is well-known (e.g., [Gor16, Prop. 1]). Now, two pairs (c_1, d_1) and (c_2, d_2) lead to the same function if and only if, for all $x \in \mathbb{F}_2^n$,

$$F(x \oplus c_1) \oplus F(x \oplus c_2) = d_1 \oplus d_2 ,$$

which means that $\Delta_{c_1 \oplus c_2} F = d_1 \oplus d_2$, i.e. $(c_1 \oplus c_2)$ is a linear structure and $d_2 = d_1 \oplus \Delta_{c_1 \oplus c_2} F$. Then, the number of distinct functions $F_{c,d}$ equals $2^{2n-\ell}$. □

In the sequel, we consider that two functions are trivially DDT-equivalent if they satisfy Equation (1) from the above Proposition 2. Moreover, we say that a DDT-equivalent class is *trivial* if its size matches the lower-bound given in Proposition 2.

In [Gor16], Gorodilova conjectures that if F is an APN quadratic function, then for all functions F' that are DDT-equivalent to F we have that $\deg(F \oplus F') \leq 1$. This relation is obvious if F' is trivially equivalent to F as in this case $F \oplus F'$ is just a derivative function of F. However, the above relation does not hold if F is not APN. The following proposition exhibits such a counter-example.

Proposition 3. *For any even $n \geq 4$, there exists a quadratic function Q from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ whose DDT-equivalence class contains a function of any degree d, $2 \leq d \leq n/2$.*

Proof. Let f be a bent function of n variables and F be the function from $\mathbb{F}_2^n$ into itself defined by

$$F(x) = (f(x), c_1, \ldots, c_{n-1}), \forall x \in \mathbb{F}_2^n ,$$

where $(c_1, \ldots, c_{n-1})$ is a constant in $\mathbb{F}_2^{n-1}$. Then, $\Delta_a F(x) = (\Delta_a f(x), 0, \ldots, 0)$. Since f is bent, $\Delta_a f$ is balanced for all nonzero a. Then, $\Delta_a F$ takes the value $(0, 0, \ldots, 0)$ for 2^{n-1} inputs, and the value $(1, 0, \ldots, 0)$ for the other ones. In other words, the DDT of any such Sbox F is defined by: for any nonzero $a \in \mathbb{F}_2^n$,

$$\delta(a, 00\ldots0) = \delta(a, 10\ldots0) = 2^{n-1} \text{ and } \delta(a, b) = 0, \forall b \notin \{0\ldots0, 10\ldots0\}$$

$$\delta(0\ldots0, 0\ldots0) = 2^n \text{ and } \delta(0\ldots0, b) = 0 \text{ for all nonzero } b .$$

The result then follows from the fact that, for any even $n \geq 4$, there exist bent functions of n variables with degree d for all $2 \leq d \leq n/2$ [Rot76, Page 303]. □

For instance, the following quadratic Sbox F from $\mathbb{F}_2^4 \to \mathbb{F}_2^4$ follows the previous construction

$$F = [\texttt{1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1}].$$

The DDT class of F is not trivial and contains 7168 functions. This number actually corresponds to the number of bent functions of 4 variables, 28×2^5, multiplied by the number of possible constants $(c_1, c_2, c_3) \in \mathbb{F}_2^3$ that can be used for defining the last three coordinates. As an example,

$$F' = [\texttt{1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1}].$$

is non-trivially DDT-equivalent to F and has also algebraic degree two. However, $\deg(F \oplus F') = 2$.

As we have just shown, the DDT-equivalence does not preserve the algebraic degree. Another natural question is what happens with the differential uniformity. Obviously, the DDT-equivalence preserves the differential uniformity. However, this is not the case for γ-equivalence. We give below a four functions $F_1, \dots, F_4$ from $\mathbb{F}_2^4$ to itself that are γ-equivalent but have a different differential uniformity.

$$\begin{aligned}
F_1 &= \texttt{[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]} \text{ with } \delta_{F_1} = 14,\\
F_2 &= \texttt{[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1]} \text{ with } \delta_{F_2} = 12,\\
F_3 &= \texttt{[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1]} \text{ with } \delta_{F_3} = 10,\\
F_4 &= \texttt{[1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1]} \text{ with } \delta_{F_4} = 8.
\end{aligned}$$

The last function, F_4, has degree two. Since F_1, F_2, F_3 are γ-equivalent to F_4 but not DDT-equivalent, F_4 is an example of a quadratic function whose γ-equivalence class does not coincide with the DDT-equivalence class.

2.3 Invariance of the Sizes of Differential-Equivalence Classes Under CCZ-Equivalence

Another important property of the size of these equivalence classes is the following result proved in [Gor16] for γ-equivalence, which can easily be generalized to DDT-equivalence. The proof, that closely follows the proof idea of [Gor16] is provided here for completeness.

Proposition 4 (adapted from [Gor16]). *Let F and G be two functions which are EA-equivalent, i.e., there exist three affine functions A_0, A_1, A_2 where A_1 and A_2 are bijective such that $G = A_2 \circ F \circ A_1 \oplus A_0$. Then, the DDT-equivalence classes (resp. γ-equivalence classes) of F and of G have the same size. Moreover, the class of G is composed of all $A_2 \circ F' \circ A_1 \oplus A_0$ where F' varies in the class of F.*

Proof. Let L_0, L_1 and L_2 denote the linear parts of the affine functions A_0, A_1 and A_2. It is well-known that the DDT of F and G are related by

$$\delta_G(a,b) = \delta_F(L_1(a), L_2^{-1}(b \oplus L_0(a))), \text{ for all } (a,b)\ . \tag{2}$$

This comes from the fact that

$$\begin{aligned}
\varDelta_a G(x) &= A_2[F(A_1(x \oplus a))] \oplus A_2[F(A_1(x))] \oplus A_0(x \oplus a) \oplus A_0(x),\\
&= L_2\left[F(A_1(x) \oplus L_1(a)) \oplus F(A_1(x))\right] \oplus L_0(a),\\
&= L_2\left[\varDelta_{L_1(a)} F(A_1(x))\right] \oplus L_0(a).
\end{aligned}$$

Let $F' \in \mathcal{C}_{\mathsf{DDT}}(F)$ be an element in the DDT-equivalence class of F and let us consider $G' = A_2 \circ F' \circ A_1 \oplus A_0$. Then, the DDT of F' and G' satisfy: for all (a,b)

$$\delta_{G'}(a,b) = \delta_{F'}(L_1(a), L_2^{-1}(b \oplus L_0(a))) = \delta_F(L_1(a), L_2^{-1}(b \oplus L_0(a))),$$

where the last equality comes from the fact that F and F' have the same DDT. Then, we deduce from (2) that $\delta_{G'}(a,b) = \delta_G(a,b)$ for all (a,b). It follows that

$$\left\{(A_2 \circ F' \circ A_1 \oplus A_0), F' \in \mathcal{C}_{\mathsf{DDT}}(F)\right\} \subseteq \mathcal{C}_{\mathsf{DDT}}(G).$$

By exchanging the roles of F and G, we deduce that both sets coincide. □

Whether an analogue of the previous result holds for CCZ-equivalence is a natural question raised by Gorodilova [Gor16]. An obvious case for which it can be proved that two CCZ-equivalent functions F and G have DDT-classes of the same size is when F is a permutation and $G = F^{-1}$. Indeed, if F is a permutation, any function Φ in $\mathcal{C}_{\mathsf{DDT}}(F)$ is a permutation too and the DDT of Φ^{-1} satisfies

$$\delta_{\Phi^{-1}}(a,b) = \delta_{\Phi}(b,a) = \delta_F(b,a) = \delta_{F^{-1}}(a,b).$$

Thus, $\mathcal{C}_{\mathsf{DDT}}(F^{-1}) = \{\Phi^{-1}, \Phi \in \mathcal{C}_{\mathsf{DDT}}(F)\}$. But the general case of two CCZ-equivalent functions F and G seems more difficult. Indeed, CCZ-equivalence means that $\{(x, G(x)), x \in \mathbb{F}_2^n\}$ is the image of $\{(x, F(x)), x \in \mathbb{F}_2^n\}$ by a linear permutation $\mathcal{L}$ of $\mathbb{F}_2^n \times \mathbb{F}_2^n$. However, this implies that, if $\mathcal{L}$ is seen as a pair of functions, $\mathcal{L} : (x, y) \mapsto (L_1(x, y), L_2(x, y))$, then $x \mapsto L_1(x, F(x))$ is a permutation. This last condition is then required for transforming a given function F into a CCZ-equivalent function. Thus, if we want to prove, as it holds when F and G are EA-equivalent, that the DDT-equivalence class of F can be transformed into the DDT-equivalence of G by applying the same $\mathcal{L}$, we need to prove that $x \mapsto L_1(x, \Phi(x))$ is a permutation for all $\Phi \in \mathcal{C}_{\mathsf{DDT}}(F)$. This is the keypoint in the following theorem.

Theorem 1. *Let F and G be two CCZ-equivalent functions from $\mathbb{F}_2^n$ into itself and let $\mathcal{L}$ be a linear permutation of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ seen as a pair of two linear functions: $\mathcal{L}(x, y) = (L_1(x, y), L_2(x, y))$ such that $F_1 : x \mapsto L_1(x, F(x))$ is a permutation and*

$$\mathcal{L}(x, F(x)) = (F_1(x), G \circ F_1(x)) \text{ for all } x \in \mathbb{F}_2^n.$$

Then, the DDT-equivalence classes (resp. γ-equivalence classes) of F and of G have the same size. More precisely,

$$\mathcal{C}_{\mathsf{DDT}}(G) = \left\{L_2(\Phi_1^{-1}(x), \Phi \circ \Phi_1^{-1}(x)),\ \Phi \in \mathcal{C}_{\mathsf{DDT}}(F)\right\},$$
$$\mathcal{C}_{\gamma}(G) = \left\{L_2(\Phi_1^{-1}(x), \Phi \circ \Phi_1^{-1}(x)),\ \Phi \in \mathcal{C}_{\gamma}(F)\right\},$$

where $\Phi_1 : x \mapsto L_1(x, \Phi(x))$.

Proof. The proof results from the fact that the DDT of two CCZ-equivalent functions F and G, which are related by

$$\mathcal{L}(x, F(x)) = (F_1(x), G \circ F_1(x)) \text{ for all } x \in \mathbb{F}_2^n,$$

satisfy:

$$\delta_G(a,b) = \delta_F(\mathcal{L}^{-1}(a,b)) \text{ for all } (a,b).$$

Indeed, the number of (x, x') in $\mathbb{F}_2^n$ such that

$$x \oplus x' = a \text{ and } G(x) \oplus G(x') = b$$

equals the number of $y = F_1^{-1}(x)$ and $y' = F_1^{-1}(x')$ such that

$$F_1(y) \oplus F_1(y') = a \text{ and } G \circ F_1(y) \oplus G \circ F_1(y') = b$$

or equivalently

$$\mathcal{L}(y, F(y)) \oplus \mathcal{L}(y', F(y')) = \mathcal{L}\left(y \oplus y', F(y) \oplus F(y')\right) = (a, b).$$

It follows that, for any $\Phi \in \mathcal{C}_{\mathsf{DDT}}(F)$ such that $\Phi_1 : x \mapsto L_1(x, \Phi(x))$ is a permutation, the function $\Gamma : x \mapsto L_2(\Phi_1^{-1}(x), \Phi \circ \Phi_1^{-1}(x))$ satisfies

$$\delta_\Gamma(a, b) = \delta_\Phi(\mathcal{L}^{-1}(a, b)) = \delta_F(\mathcal{L}^{-1}(a, b)),$$

where the first equality is deduced from the fact that

$$\mathcal{L}(x, \Phi(x)) = (\Phi_1(x), \Gamma \circ \Phi_1(x)), \ \forall x \in \mathbb{F}_2^n.$$

Thus, $\delta_\Gamma(a, b) = \delta_G(a, b)$, i.e. $\Gamma \in \mathcal{C}_{\mathsf{DDT}}(G)$. Similarly, for any $\Phi \in \mathcal{C}_\gamma(F)$ such that $\Phi_1 : x \mapsto L_1(x, \Phi(x))$ is a permutation, the indicators of the DDTs satisfy

$$\gamma_\Gamma(a, b) = \gamma_\Phi(\mathcal{L}^{-1}(a, b)) = \gamma_F(\mathcal{L}^{-1}(a, b)),$$

implying that $\Gamma \in \mathcal{C}_\gamma(G)$.

Now, we need to prove that any $\Phi \in \mathcal{C}_\gamma(F)$ is such that $\Phi_1 : x \mapsto L_1(x, \Phi(x))$ is a permutation. Suppose that Φ_1 is not a permutation. Then, there exist two distinct elements x and x' in $\mathbb{F}_2^n$ such that $L_1(x, \Phi(x)) = L_1(x', \Phi(x'))$, implying $L_1(x \oplus x', \Phi(x) \oplus \Phi(x')) = 0$. Let $a := x \oplus x'$ and $b := \Phi(x) \oplus \Phi(x')$. Then, $L_1(a, b) = 0$ and both a and b differ from 0 since Φ is a permutation. By definition, $\delta_\Phi(a, b) > 0$ since x and x' are solutions of

$$\Phi(X \oplus a) \oplus \Phi(X) = b.$$

Since $\Phi \in \mathcal{C}_\gamma(F)$, $\delta_\Phi(a, b) > 0$ if and only if $\delta_F(a, b) > 0$. We deduce that

$$\delta_G(\mathcal{L}(a, b)) = \delta_F(a, b) > 0.$$

But, $\mathcal{L}(a, b) = (L_1(a, b), L_2(a, b)) = (0, c)$ for some nonzero $c \in \mathbb{F}_2^n$ since $\mathcal{L}$ is a permutation and $(a, b) \neq (0, 0)$. We then get that there exists some nonzero c such that $\delta_G(0, c) > 0$, which is impossible. Therefore, for any $\Phi \in \mathcal{C}_\gamma(F)$, $x \mapsto L_1(x, \Phi(x))$ is a permutation. We deduce that

$$\left\{L_2(\Phi_1^{-1}(x), \Phi \circ \Phi_1^{-1}(x)), \ \Phi \in \mathcal{C}_{\mathsf{DDT}}(F)\right\} \subseteq \mathcal{C}_{\mathsf{DDT}}(G)$$

and $|\mathcal{C}_{\mathsf{DDT}}(G)| \geq |\mathcal{C}_{\mathsf{DDT}}(F)|$. Similar relations hold for the γ-equivalence classes. Equality is then derived by exchanging the roles of F and G. □

It follows that the sizes of these differential-equivalence classes can be computed for one representative in each CCZ-equivalence class only.

2.4 Other Characterizations of DDT-Equivalence

The DDT-equivalence can also be expressed in terms of the Walsh transform. Indeed, it is well-known [CV95, BN13] that the squared Walsh coefficients of an Sbox are obtained by computing the Fourier transform of its difference table.

Definition 4 (Walsh transform). *Let F be a function from F_2^n into itself. The* Walsh transform of F *is the function*

$$\mathcal{W}_F : (u, v) \mapsto \mathcal{W}_F(u, v) = \sum_{x \in \mathbb{F}_2^m} (-1)^{u \cdot x + v \cdot F(x)},$$

where $x \cdot y$ denotes the scalar product between two elements x and y in $\mathbb{F}_2^n$.

Proposition 5 (DDT-equivalence and Walsh transform). *Let F and G be two functions from $\mathbb{F}_2^n$ into itself. Then, F and G are DDT-equivalent if and only if*

$$\mathcal{W}_F^2(u, v) = \mathcal{W}_G^2(u, v),\ \forall u, v \in \mathbb{F}_2^n.$$

Proof. The squared Walsh coefficients of any function are given by applying the Walsh transform to the difference table as follows (see e.g. [BN13]): for any $u, v \in \mathbb{F}_2^n$,

$$\mathcal{W}_F^2(u, v) = \sum_{a, b \in \mathbb{F}_2^n} (-1)^{a \cdot u + b \cdot v} \delta_F(a, b). \tag{3}$$

Therefore, if F and G have the same DDT, we deduce that

$$\mathcal{W}_F^2(u, v) = \mathcal{W}_G^2(u, v),\ \forall u, v \in \mathbb{F}_2^n.$$

The converse is derived in the same way, since applying the inverse Fourier transform to (3) leads to

$$\delta_F(a, b) = 2^{-2n} \sum_{u, v \in \mathbb{F}_2^n} (-1)^{a \cdot u + b \cdot v} \mathcal{W}_F^2(u, v).$$

□

The size of the DDT-equivalence class of a function then corresponds to the number of sequences of signs which provide a valid Walsh transform from a given squared Walsh transform.

The DDT-equivalence can also be characterized by the Hamming weights of the derivatives of the components of the Sbox, as stated in the following proposition.

Proposition 6. *Let F and G be two functions from $\mathbb{F}_2^n$ into itself. Then, F and G are DDT-equivalent if and only if, for all $v \in \mathbb{F}_2^n$, the Boolean functions $F_v : x \mapsto v \cdot F(x)$ and $G_v : x \mapsto v \cdot G(x)$ are such that $\Delta_a F_v$ and $\Delta_a G_v$ have the same Hamming weight for all $a \in \mathbb{F}_2^n$.*

Proof. Let v be a nonzero element in $\mathbb{F}_2^n$. Then,

$$\begin{aligned}
2^n - wt(\Delta_a F_v) &= \#\left\{x \in \mathbb{F}_2^n : \Delta_a F_v(x) = 0\right\} \\
&= \#\left\{x \in \mathbb{F}_2^n : v \cdot \Delta_a F(x) = 0\right\} \\
&= \#\left\{x \in \mathbb{F}_2^n : \Delta_a F \in \langle v \rangle^\perp\right\} \\
&= \sum_{b \in \langle v \rangle^\perp} \delta_F(a, b).
\end{aligned}$$

It follows that, if F and G have the same DDT, then

$$wt(\Delta_a F_v) = wt(\Delta_a G_v), \forall a \in \mathbb{F}_2^n \ .$$

Obviously, the equality also holds when $v = 0$ since F_0 and G_0 both correspond to the all-zero function in this case.

Conversely, let us now assume that $wt(\Delta_a F_v) = wt(\Delta_a G_v)$ for all a and v. It is known (e.g., [Car93]) that

$$\mathcal{W}_F^2(u,v) = \sum_{a \in \mathbb{F}_2^n} (-1)^{a \cdot u} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{\Delta_a F_v(x)} \right) .$$

Using that

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{\Delta_a F_v(x)} = 2^n - 2wt(\Delta_a F_v),$$

we deduce that, for all $u, v \in \mathbb{F}_2^n$,

$$\mathcal{W}_F^2(u,v) = \mathcal{W}_G^2(u,v),$$

which is equivalent to F and G being DDT-equivalent. □

Applying the previous characterization to quadratic functions leads to the following corollary.

Corollary 1. *Let F and G be two quadratic functions from $\mathbb{F}_2^n$ into itself. Then, F and G are DDT-equivalent if and only if, for any $v \in \mathbb{F}_2^n$, F_v and G_v have the same linear space LS_v and, for any $a \in LS_v$, $\Delta_a F_v = \Delta_a G_v$.*

Proof. The proof is directly derived from the previous proposition, using the fact that, for a quadratic Boolean function f, any a which is not a linear structure of f is such that $\Delta_a f$ has degree one implying that $wt(\Delta_a f) = 2^{n-1}$. Therefore, the fact that $\Delta_a F_v$ and $\Delta_a G_v$ have the same Hamming weight needs to be checked when a is a linear structure of F_v and G_v only. □

3 Computation of the γ-Equivalence and DDT-Equivalence Classes

We present in this section an algorithm that takes as input a $2^n \times 2^n$ table D filled with nonnegative integers and returns all functions F from $\mathbb{F}_2^n$ into itself, if any, whose difference distribution table has the same indicator (see Definition 3) as the one of D, which we denote γ_D. In other words, our algorithm retrieves the γ-equivalence class of functions of a given table D. Note that one can also derive the DDT-equivalent functions from this class, by post-filtering the functions returned by the algorithm against a desired DDT.

Throughout the following sections, we denote binary vectors of $\mathbb{F}_2^n$ by integers and make an extensive use of this notation. The algorithm determines all possible values for $F(i)$, $i = 0, \ldots, 2^n - 1$, by taking into account the constraints imposed by the table D and the values $F(j)$, $j < i$, that have already been computed. It essentially implements a tree-traversal algorithm, where each Level i contains the nodes corresponding to the possible values that $F(i)$ can take. The tree therefore has depth 2^n. There is a natural incentive to implement such algorithms using recursion, which we adopt in the sequel.

From now on, we denote by $\mathcal{R}_i = \{y : D[i][y] \neq 0\}$ the set of column indices of non-zero elements on D's ith row. The algorithm starts running and tries to determine all possible values for $F(0), F(1), \ldots, F(2^n - 1)$. By assuming that all values $F(0)$, $F(1)$, . . . , $F(i-1)$ have already been set, the value $F(i)$ can be computed according to the following relations:

- $F(i) \oplus F(0) = \Delta_i F(0)$ must lie in $\mathcal{R}_i$,
- $F(i) \oplus F(1) = \Delta_{i\oplus 1} F(1)$ must lie in $\mathcal{R}_{i\oplus 1}$,
- $F(i) \oplus F(2) = \Delta_{i\oplus 2} F(2)$ must lie in $\mathcal{R}_{i\oplus 2}$,
- ...
- $F(i) \oplus F(i-1) = \Delta_{i\oplus(i-1)} F(i-1)$ must lie in $\mathcal{R}_{i\oplus(i-1)}$.

Thus, $F(i)$ should lie in the intersection of the sets

$$\{x \oplus F(0) : x \in \mathcal{R}_i\} \cap \{x \oplus F(1) : x \in \mathcal{R}_{i\oplus 1}\} \cap \cdots \cap \{x \oplus F(i-1) : x \in \mathcal{R}_{i\oplus(i-1)}\}.$$

If this intersection is empty, then the algorithm backtracks and picks another value for $F(i-1)$, from the set of possible values. Otherwise, $F(i)$ is set to the smallest element in the intersection and the algorithm continues by searching for possible values for $F(i+1)$. At this point, it has to be noticed that $F(0)$ can take any given value. However, we explain now a pruning observation that prevents the algorithm from trying all possible 2^n values for $F(0)$ and all possible values for $F(1)$.

Pruning. We can reduce the search space of the algorithm by pruning some branches. The procedure starts, without restriction, by the determination of the images of 0 and 1. We explain now why it is possible to fix those two values and still recover all the other functions for different values of these images.

First, recall that a function $F(x)$ and $F(x) \oplus d$, for any $d \in \mathbb{F}_2^n$, have the same DDT. This implies that there are at least 2^n functions having a certain DDT for any image of 0. We can therefore fix the image of 0 to any particular value, and query the algorithm for functions having this first defined point. All the other functions will then be recovered by translation.

Second, for a defined image of 0, it is not necessary to ask the algorithm to look for every possible image of 1. Indeed, the functions $F(x)$ and $F(x \oplus c) \oplus F(0) \oplus F(c)$, for any $c \in \mathbb{F}_2^n$, have the same DDT. This means that, once $F(0)$ has been fixed, there are as many solutions for any value of $F(1)$ as long as $F(0) \oplus F(1) \in \mathcal{R}_1$. Moreover, remark that there is an even number of functions having the same DDT and the same images in 0 and 1: the functions $F(x)$ and $F(x \oplus 1) \oplus F(0) \oplus F(1)$ are equal in 0 and 1.

One Example. Before giving the pseudo-code of the algorithm, we show a small example of its execution for the $2^3 \times 2^3$ table shown in Figure 1, which corresponds to the DDT of the PRINTcipher Sbox [KLPR10].

Here are the main steps performed by the algorithm (also see Figure 2):

1. Set $F(0) = 0$
2. Set $F(1) = 1$, as 1 is the minimal value of the set $\mathcal{R}_1 = \{1, 3, 5, 7\}$

		Δ_{out}							
		0	1	2	3	4	5	6	7
	0	8	.	.	.	.	.	.	.
	1	.	2	.	2	.	2	.	2
	2	.	.	2	2	.	.	2	2
Δ_{in}	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

Figure 1: Difference distribution table of dimension $2^3 \times 2^3$ corresponding to the PRINTcipher Sbox.

3. As $F(2) \oplus F(0) \in \mathcal{R}_2 = \{2,3,6,7\}$ and $F(2) \oplus F(1) \in \mathcal{R}_3 = \{1,2,5,6\}$, $F(2) \in \{2,3,6,7\} \cap \{0,3,4,7\} = \{3,7\}$. Set $F(2) = 3$.
4. As $F(3) \oplus F(0) \in \mathcal{R}_3 = \{1,2,5,6\}$, $F(3) \oplus F(1) \in \mathcal{R}_2 = \{2,3,6,7\}$ and $F(3) \oplus F(2) \in \mathcal{R}_1 = \{1,3,5,7\}$, $F(3) \in \{1,2,5,6\} \cap \{2,3,6,7\} \cap \{0,2,4,6\} = \{2,6\}$. Set $F(3) = 2$.
5. As $F(4) \oplus F(0) \in \mathcal{R}_4 = \{4,5,6,7\}$, $F(4) \oplus F(1) \in \mathcal{R}_5 = \{1,3,4,6\}$, $F(4) \oplus F(2) \in \mathcal{R}_6 = \{2,3,4,5\}$ and $F(4) \oplus F(3) \in \mathcal{R}_7 = \{1,2,4,7\}$, $F(4) \in \{4,5,6,7\} \cap \{0,2,5,7\} \cap \{0,1,6,7\} \cap \{0,3,5,6\} = \emptyset$.
6. Go back to Step 4 and set $F(3) = 6$. Compute now any possible values for $F(4)$ by repeating Step 5, with $F(3) = 6$.
7. ...
8. Once $F(7)$ has been fixed, we verify that γ_F is equal to the indicator of D and add it to a list of *solutions*. We then backtrack to find the other solutions.

The two solutions found with the restrictions $F(0) = 0$ and $F(1) = 1$ are $F = (0,1,3,6,7,4,5,2)$ and $F' = (0,1,7,2,5,6,3,4)$ as it can be seen in Figure 2. All the γ-equivalent functions can be found by computing $F(x \oplus c) \oplus d$ and $F'(x \oplus c) \oplus d$ for all $c, d \in \mathbb{F}_2^3$. At the end, we obtain 2^6 γ-equivalent functions.

Algorithm. In the algorithm, we take the pruning observation into account and only look for functions such that the image of 0 is 0 and the image of 1 is the first possible value. From now on, we denote by S a table of dimension 2^n used to store the intermediate possible images. Then, we denote by F a solution returned by the algorithm, obtained when all the cells of S have been set.

Hence, at the beginning, $S[0]$ is set to 0 and $S[1]$ is set to $\min\{\mathcal{R}_1\}$. The recursive Algorithm 2 is then called for $i = 2$, where i means that the algorithm is searching for candidate values for $S[i]$. It starts by computing the possible values for $S[i]$ on Line 2 and store them in a set $\mathcal{L}$. If this set is not empty, the algorithm tries to compute the next value, $S[i+1]$, for every possible value of $S[i]$. The procedure is repeated until either $S[2^n - 1]$ has been set or $\mathcal{L}$ is empty. In the latter case, the algorithm backtracks to the next possible value in $\mathcal{L}$ at a certain Level i as there was no solution in this branch. In the former case, all the values for S have been set. At this point, we verify (Line 4) whether the function found has the same γ indicator as the table D (resp. it has D as a DDT). Indeed, it is possible that the support of γ_S is strictly included in the one of the indicator of D.

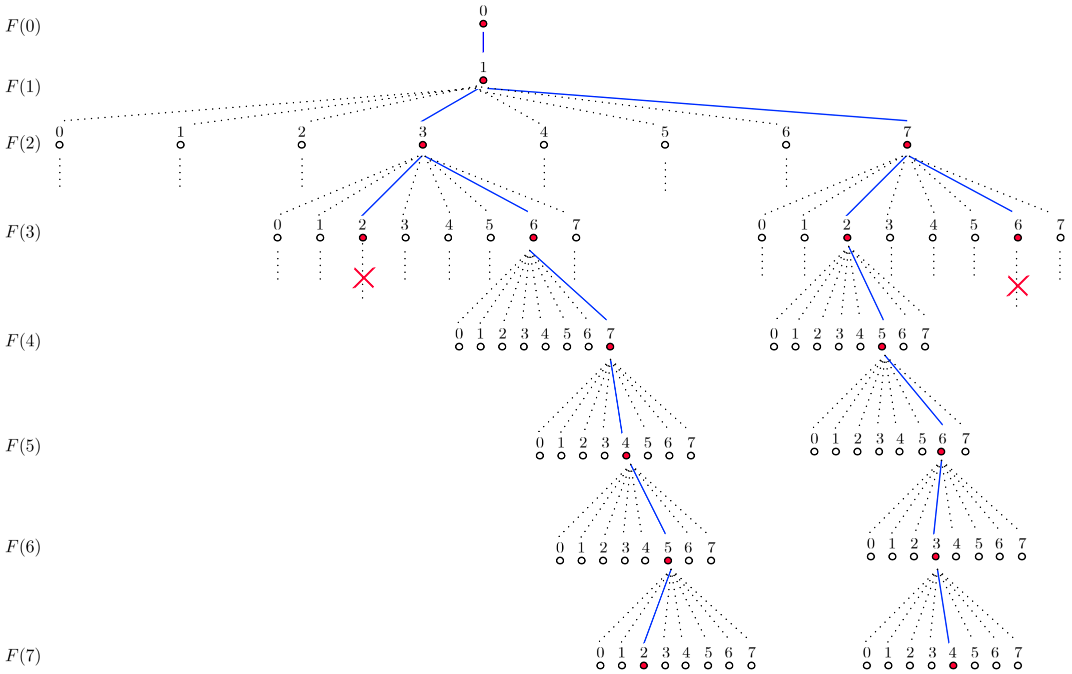

Figure 2: Example of the algorithm's execution on the table of Figure 1.

Algorithm 1 `Main`

Input: A table D of size $2^n \times 2^n$

Output: A list $\mathcal{F}$ of all functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ γ-equivalent to the indicator of D

```
$\mathcal{F} \leftarrow \{\emptyset\}$                                  ▷ Globaly defined
$S \leftarrow [0, \min\{\mathcal{R}_1\}, 0, \ldots, 0]$                    ▷ len($S$) $= 2^n$
RecursifSearch($S, 2$)
return $\mathcal{F}$
```

4 Experimental Results

One of the questions we are interested in is the existence of two DDT-equivalent permutations F and G, which are not related by $G(x) = F(x \oplus c) \oplus d$ for some c, d. It is worth noticing that, in the case of non-bijective mappings, such pairs of functions exist. For instance, in [Gor16], $2^{2n+n/2}$ quadratic functions have been exhibited, which are γ-equivalent (and thus DDT-equivalent) to the Gold function $x^{2^{n/2+1}+1}$ over $\mathbb{F}_{2^n}$ when n is a multiple of 4.

4.1 Results for some Known Functions

Using the algorithm described in the previous section, we have been able to compute the γ-equivalence classes and the DDT-equivalence classes of some cryptographically relevant functions. It is clear from Theorem 1, that it is sufficient to run the algorithm for a single representative in each CCZ-equivalence class.

Known APN Permutations for $n \leq 9$. After computation, we can affirm that the size of the DDT-equivalence classes of all known APN permutations over $\mathbb{F}_2^n$, with $n \leq 9$, is 2^{2n}. This equivalently means that each DDT-equivalence class is trivial.

Algorithm 2 `RecursifSearch`

```
Input: A table $S$ of size $2^n$, an integer $i$
if $i < 2^n$ then
    $\mathcal{L} \leftarrow \bigcap_{0 \leq k < i} \{x \oplus S[k] : x \in \mathcal{R}_k\}$
else
    if $\gamma_S = \gamma_D$ then                ▷ Or DDT($S$) = $D$ if we test the DDT-equivalence
        Append $S$ to $\mathcal{F}$
    return
if $\mathcal{L} \neq \emptyset$ then
    for all $x \in \mathcal{L}$ do
        $S[i] \leftarrow x$
        RecursifSearch($S, i + 1$)
else
    return
```

More precisely, for $n \leq 9$, the known classes of APN permutations can be defined, up to CCZ equivalence, by the following representatives:

- for $n = 3$: the Gold permutation,
- for $n = 5$: the three CCZ-classes described by Brinkmann and Leander in [BL08, Table 3],
- for $n = 6$: the so-called Dillon permutation [BDMW10],
- for $n \in \{7, 9\}$: the power permutations given in [BDKM09, Table 1].

For $n \leq 8$, all known quadratic APN functions have been studied by Gorodilova (see Table 4 in [Gor16]). Here, we also checked that the DDT-equivalence classes of all known APN permutations of degree strictly higher than two are trivial. It is worth noticing that all known APN permutations in dimension 6 are CCZ-equivalent to a quadratic function [BDMW10]. The fact that the corresponding DDT-equivalent class is trivial is then directly deduced from Theorem 1 and [Gor16].

APN Functions for $n \leq 8$. We also carried out some experiments for non-bijective APN functions. For instance, we can easily compute the sizes of the DDT-equivalence classes of all APN functions of 6 variables of degree at most 3. Indeed, there exist 21 CCZ-equivalence classes of APN functions of 6 variables of degree at most 3 [Lan09] but all these classes contain a quadratic function, except the class discovered independently by [EP09] and by [BL08]. Since Gorodilova has computed the sizes of the DDT-equivalence classes for all quadratic APN functions in six variables, we only need to consider the single remaining class, named Class 13 in [BL08, Table 5]. We have computed the DDT-equivalence class of this function and seen that it is trivial.

Furthermore, we have computed the sizes of the DDT-equivalence classes for all APN functions of 7 and 8 variables given in [BDKM09]. We found that all of the given functions in dimension 7 have trivial classes, while in dimension 8 only the function x^9 has a not trivial class containing 2^{20} functions as proved in [Gor16, Theorem 1].

Optimal Sboxes for $n = 4$. We have also examined all permutations of dimension $n = 4$ with optimal differential uniformity (equal to 4) and optimal nonlinearity from the 16 different affine-equivalence classes given in [LP07]. The γ-equivalence class for each of them contains exactly 2^8 elements. Since none of these functions has a linear structure, we deduce from Proposition 2 that these 2^8 elements also form their DDT-equivalence class.

As we have seen, none of the permutations with the lowest possible differential uniformity in dimension $n < 6$ has a DDT-equivalence class with size bigger than 2^{2n}. However, it is possible to construct such permutations when we increase the differential uniformity.

4.2 An Example of Non-Trivially DDT-Equivalent Permutations

In this paragraph, we exhibit a permutation F over $\mathbb{F}_2^5$, such that some elements in its DDT-equivalence class are not of the form $F(x \oplus c) \oplus d$ for any $c, d \in \mathbb{F}_2^5$.

We consider the table D, composed by 2×2 blocks of the form $\begin{bmatrix} 16 & 16 \\ 16 & 16 \end{bmatrix}$ everywhere on the diagonal except for the first block which is $\begin{bmatrix} 32 & 0 \\ 0 & 32 \end{bmatrix}$. By running our algorithm on this table, we recovered 56×2^8 permutations having this DDT. Even by considering the fact that the permutations corresponding to this DDT will necessarily have a linear structure, this number is still higher than the number of distinct functions of the form $F(x \oplus c) \oplus d$, which equals $2^{2 \times 5 - 1}$ as shown in Proposition 2.

In Table 1 are presented two functions F and F' whose DDT is D but for which there is no pair (c, d) such that $F'(x) = F(x \oplus c) \oplus d$ for all x.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$F(x)$	0	1	2	3	4	5	6	7	8	9	10	11	13	12	15	14
$F'(x)$	0	1	2	3	4	5	6	7	8	9	10	11	13	12	15	14
x	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$F(x)$	16	17	19	18	20	21	23	22	25	24	26	27	28	29	31	30
$F'(x)$	16	17	19	18	21	20	22	23	24	25	27	26	28	29	31	30

Table 1: Two non-trivially DDT-equivalent permutations.

4.3 A Conjecture on the Size of DDT-Equivalence Classes

Several examples of functions having a non-trivial DDT-equivalence class are now known. They include some non-bijective APN functions in even dimension, namely the Gold functions for $n \equiv 0 \bmod 4$ [Gor16] and a quadratic APN function in six variables (Number 12 in Table 5 in [BL08]), and the examples exhibited in this paper. The common point between all these examples is that they have non-distinct rows in their DDTs. Besides this property, they seem to have very different characteristics: some of them are permutations with a linear structure, while the other ones are non-bijective and APN. Moreover, as previously noticed, the APN permutations seem to not have larger DDT-equivalence classes (at least for small dimensions).

These remarks, combined with the computations we have performed using our algorithm, lead us to the statement of the following conjecture.

Conjecture 1. The DDT-equivalence class of a permutation F, such that the rows in its DDT are pairwise distinct, only contains permutations of the form $F(x \oplus c) \oplus d$, with $c, d \in \mathbb{F}_2^n$ (i.e. is trivial).

It is worth noticing that Example 1 shows that the same conjecture does not hold for γ-equivalence.

Hoping to make a step towards the proof of this conjecture, we show in the next section that APN permutations cannot have two equal rows in their DDTs.

5 A Note on the DDTs of APN Permutations

Since the DDTs having at least two equal rows seem to play an important role, a natural question is the following: Is it possible that this situation occurs for some remarkable families of Sboxes? As a partial answer, we prove in this section that all the rows in the DDT of any APN permutation are distinct.

Let F be an APN permutation of $\mathbb{F}_2^n$. We start by stating two simple remarks. The first remark is due to the fact that F is a permutation while the second one is a result of F being APN.

Remark 1. $F(x) \oplus F(y) \neq F(x) \oplus F(z)$, for $x, y, z \in \mathbb{F}_2^n$ pairwise distinct.

Indeed, if we suppose that for some pairwise distinct $x, y, z \in \mathbb{F}_2^n$, we have that $F(x) \oplus F(y) = F(x) \oplus F(z)$, this would imply that $F(y) = F(z)$, which is a contradiction by the fact that F is a permutation.

Remark 2. $\Delta_a F(x) \neq \Delta_a F(y)$, for $x, y, a \in \mathbb{F}_2^n$ with $y \neq \{x, x \oplus a\}$ and $a \neq 0$.

Assuming an equality between the left and the right hand-sides of the equation, would imply an equality between two images of $\Delta_a F$ not trivially equal, which cannot occur as F is APN.

Theorem 2. *Let F be an APN permutation of $\mathbb{F}_2^n$. Then, the rows of the DDT of F are pairwise distinct.*

Proof. We prove this result by contradiction. Indeed, suppose that the row of the DDT corresponding to the image set of $\Delta_a F$ equals the row corresponding to the image set of $\Delta_b F$, for some $a, b \in \mathbb{F}_2^n \setminus \{0\}$ with $a \neq b$.

The proof then tries to match the values $\Delta_a F(x)$, for $x \in \mathbb{F}_2^n$ with the values $\Delta_b F(x)$, for $x \in \mathbb{F}_2^n$ and to show that this is impossible to do. For this, we show that it is impossible to create a chain of values $x_0, x_1, \ldots, x_{2^n-1}$ such that

$$\begin{aligned} \Delta_a F(x_0) &= \Delta_b F(x_1) \\ \Delta_a F(x_1) &= \Delta_b F(x_2) \\ &\vdots \\ \Delta_a F(x_{2^n-2}) &= \Delta_b F(x_{2^n-1}). \end{aligned}$$

We start by proving the following statement by induction.

Let $x_0, \ldots, x_{k-1} \in \mathbb{F}_2^n$ such that $\Delta_a F(x_i) = \Delta_b F(x_{i+1})$ for all $0 \leq i < k-1$. Then, there are at most $2^n - 4k$ possibilities for choosing x_k such that $\Delta_a F(x_{k-1}) = \Delta_b F(x_k)$.

More precisely, x_k does not take any of the $4k$ values $x_i, x_i \oplus a, x_i \oplus b, x_i \oplus a \oplus b$, for $i = 0, \ldots, k-1$.

Basis. Let $k = 1$. Suppose that $\Delta_a F(x_0) = \Delta_b F(x_1)$. Then, the variable x_1 cannot take any of the four values $x_0, x_0 \oplus a, x_0 \oplus b$ and $x_0 \oplus a \oplus b$. Indeed, if we suppose for example that $\Delta_a F(x_0) = \Delta_b F(x_0)$, this translates to $F(x_0) \oplus F(x_0 \oplus a) = F(x_0) \oplus F(x_0 \oplus b)$ which is impossible by Remark 1. We use Remark 1 to prove in the same way the impossibility of the remaining three values. Therefore, there are at most $2^n - 4$ possible values for x_1.

Inductive step. Suppose that for all $i < k$ there are at most $2^n - 4i$ possibilities for choosing x_i and that x_i cannot take any of the values in the set $\{x_j, x_j \oplus a, x_j \oplus b, x_j \oplus a \oplus b | 0 \leq j < i\}$. We show in the following that there are at most $2^n - 4k$ possibilities for choosing x_k.

We have that $\Delta_a(x_{k-1}) = \Delta_b(x_k)$. By Remark 1, we get that $x_k \neq \{x_{k-1}, x_{k-1} \oplus a, x_{k-1} \oplus b, x_{k-1} \oplus a \oplus b\}$. We show now that $x_k \notin \{x_i, x_i \oplus a, x_i \oplus b, x_i \oplus a \oplus b \,|\, 0 \leq i \leq k-2\}$. Indeed, suppose for example that $x_k = x_i$ for some $0 \leq i \leq k-2$. We have that

$$\Delta_a F(x_{i-1}) = \Delta_b F(x_i),$$
$$\Delta_a F(x_{k-1}) = \Delta_b F(x_i).$$

By adding these equations, we get that $\Delta_a F(x_{i-1}) = \Delta_a F(x_{k-1})$. By the induction hypothesis, $x_{k-1} \neq x_{i-1}$ and since F is APN we get a contradiction by Remark 2. The other contradictions are obtained in a similar way by the induction hypothesis and Remark 2.

We show now that it is impossible to construct such a sequence $x_0, \ldots, x_{2^n-1}$. Indeed, we can see, that for choosing for example a value for x_k for $k = 2^{n-2}$, there are $2^n - 4 \cdot 2^{n-2} = 0$ choices left. Therefore, we conclude that if F is an APN permutation of $\mathbb{F}_2^n$ all rows of the DDT must be pairwise distinct. □

Note however that the above result does not hold if one of the two conditions is not met, i.e. if F is not APN or if it is not bijective. Indeed, the two functions of Table 1 are both bijective but have equal rows in their DDT. On the other hand, Function 12 in Table 5 in [BL08] is an APN function of 6 variables whose DDT has some identical rows. Actually, this property holds for any APN quadratic function of an even number of variables.

6 Conclusion

In this paper, we investigated two different notions of differential equivalence, the DDT-equivalence and the γ-equivalence, and provided an algorithm to compute both equivalence classes for a given vectorial Boolean function. We plan to incorporate this algorithm into the recent `C++` library dedicated to the study of equivalence of Boolean functions [FJ18]. During our experiments, we encountered permutations over $\mathbb{F}_2^n$ whose differential equivalence class contains more than 2^{2n} elements. We conjectured in this paper that functions having a non-trivial DDT-equivalence class may relate to the number of distinct rows in their DDT. Furthermore, some other questions about the size of the DDT-equivalence and the γ-equivalence classes naturally arose during this work. For example, we were not able to find an example of an APN function in an odd number of variables having a non-trivial γ-equivalence class. The question is then if such APN functions exist. Another question is whether there exist differentially 4-uniform permutations whose DDT-equivalence class is different from its γ-equivalence class. We have found examples of differentially 4-uniform non-bijective functions for which the two associated classes are different, but in the bijective case, for all the tested functions, the two notions coincide. Finally, an interesting future direction would be to study the differential equivalence classes, and in particular the sizes, of functions either in higher dimensions and/or without any particular structure.

References

BCC10. Céline Blondeau, Anne Canteaut, and Pascale Charpin. Differential properties of power functions. *IJICoT*, 1(2):149–170, 2010.

BDKM09. K. Browning, J. Dillon, R. Kibler, and M. McQuistan. APN polynomials and related codes. *J. Comb. Inf. Syst. Sci.*, 34(1-4):135–159, 2009.

BDMW10. K.A. Browning, J.F. Dillon, M.T. McQuistan, and A.J. Wolfe. An APN permutation in dimension six. In *Finite Fields: Theory and Applications*, volume 518 of *Contemporary Mathematics*, pages 33–42. AMS, 2010.

BG11. Céline Blondeau and Benoît Gérard. Multiple differential cryptanalysis: Theory and practice. In Antoine Joux, editor, *FSE 2011*, volume 6733 of *LNCS*, pages 35–54. Springer, Heidelberg, February 2011.

BL08. Marcus Brinkmann and Gregor Leander. On the classification of APN functions up to dimension five. *Des. Codes Cryptography*, 49(1-3):273–288, 2008.

BN13. Céline Blondeau and Kaisa Nyberg. New links between differential and linear cryptanalysis. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 388–404. Springer, Heidelberg, May 2013.

BS91. Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. In Alfred J. Menezes and Scott A. Vanstone, editors, *CRYPTO'90*, volume 537 of *LNCS*, pages 2–21. Springer, Heidelberg, August 1991.

Car93. Claude Carlet. Partially-bent functions. *Des. Codes Cryptography*, 3(2):135–145, 1993.

Car15. Claude Carlet. Open questions on nonlinearity and on APN functions. In Çetin Kaya Koç, Sihem Mesnager, and Erkay Savaş, editors, *Arithmetic of Finite Fields - WAIFI 2014*, pages 83–107. Springer, 2015.

CCZ98. Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems. *Des. Codes Cryptography*, 15(2):125–156, 1998.

CR15. Anne Canteaut and Joëlle Roué. On the behaviors of affine equivalent sboxes regarding differential and linear attacks. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 45–74. Springer, Heidelberg, April 2015.

CV95. Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptoanalysis. In Alfredo De Santis, editor, *EUROCRYPT'94*, volume 950 of *LNCS*, pages 356–365. Springer, Heidelberg, May 1995.

Dob99. Hans Dobbertin. Almost Perfect Nonlinear Power Functions on $\mathrm{GF}(2^{\mathrm{n}})$: The Welch Case. *IEEE Transactions on Information Theory*, 45(4):1271–1275, 1999.

EKP06. Yves Edel, Gohar M.M. Kyureghyan, and Alexander Pott. A new APN function which is not equivalent to a power mapping. *IEEE Transactions on Information Theory*, 52(2):744–747, 2006.

EP09. Yves Edel and Alexander Pott. A new almost perfect nonlinear function which is not quadratic. *Adv. in Math. of Comm.*, 3(1):59–81, 2009.

FJ18. Jean-Pierre Flori and Jérémy Jean. libapn C++ Library. https://github.com/ANSSI-FR/libapn, 2018.

Gor16. Anastasiya Gorodilova. On a remarkable property of APN Gold functions. Cryptology ePrint Archive, Report 2016/286, 2016.

HM11. Fernando Hernando and Gary McGuire. Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions. *Journal of Algebra*, 343(1):78–92, 2011.

KLPR10. Lars R. Knudsen, Gregor Leander, Axel Poschmann, and Matthew J. B. Robshaw. PRINTcipher: A block cipher for IC-printing. In Stefan Mangard and François-Xavier Standaert, editors, *CHES 2010*, volume 6225 of *LNCS*, pages 16–32. Springer, Heidelberg, August 2010.

Knu95. Lars R. Knudsen. Truncated and higher order differentials. In Bart Preneel, editor, *FSE'94*, volume 1008 of *LNCS*, pages 196–211. Springer, Heidelberg, December 1995.

Lan09. Philippe Langevin. Classification of Boolean functions under the affine group. `http://langevin.univ-tln.fr/project/agl/agl.html`, 2009.

LP07. Gregor Leander and Axel Poschmann. On the Classification of 4 Bit S-Boxes. In Claude Carlet and Berk Sunar, editors, *Arithmetic of Finite Fields, First International Workshop, WAIFI 2007, Madrid, Spain, June 21-22, 2007, Proceedings*, volume 4547 of *Lecture Notes in Computer Science*, pages 159–176. Springer, 2007.

NK93. Kaisa Nyberg and Lars R. Knudsen. Provable security against differential cryptanalysis (rump session). In Ernest F. Brickell, editor, *CRYPTO'92*, volume 740 of *LNCS*, pages 566–574. Springer, Heidelberg, August 1993.

Nyb94. Kaisa Nyberg. Differentially uniform mappings for cryptography. In Tor Helleseth, editor, *EUROCRYPT'93*, volume 765 of *LNCS*, pages 55–64. Springer, Heidelberg, May 1994.

PSLL03. Sangwoo Park, Soo Hak Sung, Sangjin Lee, and Jongin Lim. Improving the upper bound on the maximum differential and the maximum linear Hull probability for SPN structures and AES. In Thomas Johansson, editor, *FSE 2003*, volume 2887 of *LNCS*, pages 247–260. Springer, Heidelberg, February 2003.

Rot76. Oscar S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory, Series A*, 20(3):300–305, 1976.

Sud15. Valentin Suder. Antiderivative functions over $\mathbb{F}_{2^n}$. In *Workshop on Coding and Cryptography - WCC 2015*, 2015.

Sud17. Valentin Suder. Antiderivative functions over $\mathbb{F}_{2^n}$. *Des. Codes Cryptography*, 82(1-2):435–447, 2017.

YWL14. Yuyin Yu, Mingsheng Wang, and Yongqiang Li. A matrix approach for constructing quadratic APN functions. *Des. Codes Cryptography*, 73(2):587–600, 2014.