On the division property of S-boxes[*]

Faruk Göloğlu [†1,2], Vincent Rijmen [‡2], and Qingju Wang [§2]

[1]Charles University Prague
[2]KU Leuven and iMinds, Belgium

Abstract

Todo introduced [20] a property of multisets of a finite field called the division property. It is then used [19] in an attack against the S7 S-box of the MISTY1 cipher. This paper provides a complete mathematical analysis of the division property. The tool we use is the discrete Fourier transform. We relate the division property to the natural concept of the degree of a subset of a finite field. This indeed provides a characterization of multisets satisfying the division property. In [18], the authors gave some properties related to the division property. In this paper we give a complete characterization and reprove many of their results. We show that the division property is actually the dual of the degree of t-products of the inverse S-box and show these two characteristics are affine invariants. We then propose a very efficient way to check vulnerability of a given S-box against attacks of this type. We also reprove some recent interesting results using the method based on the discrete Fourier transform. We finally check whether the S-boxes of the candidate ciphers in the CAESAR competition are vulnerable against attacks based on the division property.

1 Introduction

1.1 Fields and vector spaces

Let $\mathbb{F} = \mathbb{F}_{2^n}$ be the finite field with 2^n elements. Note that $\mathbb{F}$ is a vector space of dimension n over $\mathbb{F}_2$. By choosing a basis $\beta = (\beta_1, \ldots, \beta_n)$ we can easily convert an element $x \in \mathbb{F}_{2^n}$ to a vector $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ and vice versa by means of the relation

$$x = x_1\beta_1 + \cdots + x_n\beta_n.$$

We shall not make any distinction between vectors and field elements. The Hamming weight $\mathsf{wt}(\mathbf{x})$ of $\mathbf{x}$ is defined as number of $x_i \neq 1$. The binary weight of

[*]submitted on 22/10/2015

[†]farukgologlu@gmail.com

[‡]vincent.rijmen@esat.kuleuven.be

[§]qingju.wang@esat.kuleuven.be

an integer $\mathsf{wt}_2(k)$ equals the Hamming weight of the vector with the coefficients of k's expression as a sum of powers of 2. The one's complement notation implies that if $k < 2^n$ then

$$\mathsf{wt}_2(2^n - k) = n - \mathsf{wt}_2(k).$$

The trace of an element $a \in \mathbb{F}_{2^n}$ is defined as:

$$\mathsf{tr}(a) = \sum_{i=0}^{n-1} a^{2^i}.$$

1.2 Todo's division property

Todo [20] defined the following function in order to define the division property.

Definition 1 (Bit-product function)**.** Let $\mathbf{u} = (u_1, \ldots, u_n), \mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ be vectors. Then the bit-product function $\pi_{\mathbf{u}} : \mathbb{F}_2^n \to \mathbb{F}_2$ is

$$\pi_{\mathbf{u}}(\mathbf{x}) = \mathbf{x}^{\mathbf{u}} = \prod_{i=1}^{m} x_i^{u_i}.$$

Now one can define the Division property as in [20].

Definition 2 (Division property)**.** Let M be a multiset of $\mathbb{F}_2^n$. The multiset M satisfies the division property $\mathcal{D}_k^n$, if for all $\mathbf{u}$ with $\mathsf{wt}(\mathbf{u}) < k$ we have

$$\sum_{\mathbf{x} \in M} \pi_{\mathbf{u}}(\mathbf{x}) = 0.$$

One can see easily that the symmetric difference $M \bigtriangleup \{*a, a*\}$ satisfies the same division property as that of M. Therefore one can concentrate on sets instead of multisets.

Example 3. The set $\mathbb{F}_2^n$ is a $\mathcal{D}_n^n$-set.

Example 4. The hyperplanes of $\mathbb{F}_{2^n}$ are $\mathcal{D}_{n-1}^n$-sets.

2 The Discrete Fourier Transform

In this section we explain the well-known and widely used tool, the discrete Fourier transform (DFT). We will introduce the very natural concept based on the DFT of the characteristic function of a set, which we call the *degree of a set* S which is a subset of a finite field $\mathbb{F}_{2^n}$. We will then show that this concept corresponds to the division property. In this section we let $q = 2^n$.

2.1 Definition

Definition 5. The discrete Fourier transform of a function $F : \mathbb{F}_q \to \mathbb{F}_q$ is defined as

$$\tilde{F}(k) = \left\{ \begin{array}{cl} F(0) & \text{if } k = 0, \\ -\sum_{x \in \mathbb{F}_q^*} F(x)x^{-k} & \text{if } 1 \leq k \leq q-1. \end{array} \right. \tag{1}$$

It follows that

$$F(x) = \sum_{k=0}^{q-1} \tilde{F}(k)x^k \tag{2}$$

Hence, any function $F : \mathbb{F}_q \to \mathbb{F}_q$ can be written as a polynomial $F(x) \in \mathbb{F}_q[x]$. The representation is unique when one considers polynomials modulo $x^q - x$. Note that the DFT describes a way to find the polynomial $F(x)$ which uniquely corresponds to the function F. We will make no distinction between the function and the polynomial.

2.2 Degrees of functions and sets

We talk about two kinds of degrees of functions. The (usual) degree of a function $F : \mathbb{F}_q \to \mathbb{F}_q$ is the largest $0 \leq k \leq q-1$ such that $\tilde{F}(k) \neq 0$.

We can also describe F as a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. In that case, the Algebraic Normal Form (ANF) of F is

$$F(\mathbf{x}) = \sum_{\mathbf{u} \in \mathbb{F}_2^n} a_{\mathbf{u}} \pi_{\mathbf{u}}(\mathbf{x}), \tag{3}$$

with $a_{\mathbf{u}} \in \mathbb{F}_2^n$. The algebraic or Boolean degree of F (which we will call $\mathsf{deg}\,(F)$) is defined as the largest $\mathsf{wt}_2(\mathbf{u})$ such that $a_{\mathbf{u}} \neq 0$. We will be (almost exclusively) interested in the Boolean degree.

We can find $\mathsf{deg}\,(F)$ also from the DFT: $\mathsf{deg}\,(F)$ equals the largest $\mathsf{wt}_2(k)$, i.e., largest binary weight of an exponent k, such that $\tilde{F}(k) \neq 0$. See, for instance, [8] for vectorial Boolean functions and their representations. Now for a subset $S \subseteq \mathbb{F}_q$, we define the *characteristic Boolean function* $\chi_S : \mathbb{F}_q \to \mathbb{F}_2$ as

$$\chi_S(x) = \left\{ \begin{array}{ll} 1 & \text{if } x \in S, \\ 0 & \text{if } x \notin S. \end{array} \right.$$

Now it is natural to define the degree of a set:

Definition 6 (Degree of a set)**.** The degree $\mathsf{deg}\,(S)$ of a set $S \subseteq \mathbb{F}_q$ is the Boolean degree $\mathsf{deg}\,(\chi_S)$ of the characteristic Boolean function.

Now an inspection of the Eq. (1) shows that

$$\sum_{x \in S} x^k = -\tilde{\chi}_S(-k). \tag{4}$$

For a set S with $\mathsf{deg}\,(S) = d$ this means

$$\sum_{x \in S} x^k = 0$$

for all k with $\mathsf{wt}_2(k) < n - d$ and

$$\sum_{x \in S} x^k \neq 0$$

for some k with $\mathsf{wt}_2(k) = n - d$.

Note the similarity between the subsets of $\mathbb{F}_2^n$ with the division property $\mathcal{D}_d^n$ and subsets of $\mathbb{F}_{2^n}$ with degree $n - d$. The former sets satisfy $\sum_{\mathbf{x} \in S} \pi_{\mathbf{u}}(\mathbf{x}) = 0$ for all $\mathbf{u}$ with $\mathsf{wt}(\mathbf{u}) < d$, while the latter satisfies $\sum_{x \in S} x^k = 0$ for all $k < d$. We will show now that indeed these two definitions are the same. Note that we use a vector space notation for the division property and a finite field notation for the degree property. For the following we will stick to the finite field notation since the finite field $\mathbb{F}_{2^n}$ is an n-dimensional vector space over $\mathbb{F}_2$. The following lemma will be used extensively.

Lemma 7. *For any set $S \subseteq \mathbb{F}_q$ and any $F : \mathbb{F}_q \to \mathbb{F}_q$ we have*

$$B_{S,F} = \sum_{x \in S} F(x) = 0$$

if $\mathsf{deg}\,(S) + \mathsf{deg}\,(F) < n$ and for a fixed F, there exists an S with $\mathsf{deg}\,(S) = n - \mathsf{deg}\,(F)$ such that $B_{S,F} \neq 0$.

Proof. Clearly

$$B_{S,F} = \sum_{x \in S} F(x) = \sum_{x \in \mathbb{F}_q} \chi_S(x) F(x).$$

Therefore if $\mathsf{deg}\,(\chi_S) + \mathsf{deg}\,(F) < n$ then $B_{S,F} = 0$. And for any F there exists a degree $\mathsf{deg}\,(S) = n - \mathsf{deg}\,(F)$ function such that $B_{S,F} \neq 0$. Let the ANF of F have the term $A_I \prod_{i \in I} x_i$ where $I \subseteq \{1, \ldots, n\}$ and $\#I = \mathsf{deg}\,(F)$, then $\chi_S(x) = \prod_{i \notin I} x_i$ is one such function. □ □

Theorem 8. *Let S be a subset of $\mathbb{F}_q$. We have*

$$\sum_{x \in S} \pi_u(x) = 0$$

for all u with $\mathsf{wt}(u) < d$ if and only if

$$\sum_{x \in S} x^k = 0$$

for all $\mathsf{wt}_2(k) < d$.

Proof. Assume

$$\sum_{x \in S} \pi_u(x) = 0$$

for all u with $\mathsf{wt}(u) < d$. Then

$$\sum_{x \in S} \left(\prod_{i \in I} x_i \right) = 0 \tag{5}$$

for all $I \in \mathcal{P}_d^n$ where $\mathcal{P}_j^n$ is the set of all subsets I of $\{1, \ldots, n\}$ with $\#I \leq j$. For any k with $\mathsf{wt}(k) < d$ we have

$$\begin{aligned} \sum_{x \in S} x^k &= \sum_{x \in S} \left(\sum_{I \in \mathcal{P}^n_{\mathsf{wt}(k)}} \beta_I \prod_{i \in I} x_i \right) \\ &= \sum_{I \in \mathcal{P}^n_{\mathsf{wt}(k)}} \beta_I \left(\sum_{x \in S} \left(\prod_{i \in I} x_i \right) \right) \\ &= 0 \end{aligned}$$

by (5) where β_I is the corresponding coefficient determined by I in the expansion. Its value does not matter. Now assume

$$\sum_{x \in S} x^k = 0$$

for all $\mathsf{wt}_2(k) < d$. Then by (4), we have $\mathsf{deg}\,(\chi_S) \leq n - d$. And

$$\sum_{x \in S} \pi_u(x) = \sum_{x \in \mathbb{F}_q} \chi_S(x) \pi_u(x).$$

Note that since $\mathsf{deg}\,(\pi_u(x)) = \mathsf{wt}(u)$ and $\mathsf{deg}\,(\chi_S(x)\pi_u(x)) \leq n - d + \mathsf{wt}(u)$ we get

$$\sum_{x \in \mathbb{F}_q} \chi_S(x) \pi_u(x) = \sum_{x \in S} \pi_u(x) = 0$$

by Lemma 7 for all u with $\mathsf{wt}(u) < d$.

□

Corollary 9. *Let S be a subset of $\mathbb{F}_q$. Then S is a $\mathcal{D}_d^n$-set if and only if* $\mathsf{deg}\,(S) = n - d$.

3 Characteristics for S-boxes

In this section we will explain some characteristics for S-boxes regarding attacks based on the division property.

Theoretically, one can argue that an S-box is "good" if it takes input with a low complexity to output with a complexity as high as possible. Dually, output with a high complexity should come as well from input with a complexity as small as possible. The degree of a set we defined leads to these two characteristics for S-boxes. They have been used to attack the S7 S-box of MISTY1 by Canteaut and Videau [7] and Todo [19] respectively. It is a purpose of the paper to make these connections clear which we will try to do in this section.

The two characteristics explained in the previous paragraph can be written explicitly as

$$\begin{aligned} \mathsf{max}\{\mathsf{deg}\,(F(S)) \;:\; \mathsf{deg}\,(S) \leq k\}, \\ \mathsf{min}\{\mathsf{deg}\,(S) \;:\; \mathsf{deg}\,(F(S)) \geq k\}, \end{aligned}$$

for all $1 \leq k \leq n$. To have a "good" S-box, the former characteristic should be as large as possible, whereas the latter should be as small as possible.

We will show that the following two characteristics for a function $F : \mathbb{F}_q \to \mathbb{F}_q$ correspond respectively to the theoretical characteristics we have just described for an S-box.

$$\begin{aligned} \mathsf{D}_F(k) &= \mathsf{min}\{\mathsf{wt}(j) \;:\; \mathsf{deg}\left(F^j\right) \geq k\}, \\ \mathsf{C}_F(k) &= \mathsf{max}\{\mathsf{deg}\left(F^j\right) \;:\; \mathsf{wt}(j) \leq k\}, \end{aligned}$$

Theorem 10. *The characteristics* $\mathsf{C}_F(k)$ *and* $\mathsf{D}_F(k)$ *satisfy*

$$\begin{aligned} \mathsf{C}_F(k) &= n - \mathsf{min}\{\mathsf{deg}\,(S) \;:\; \mathsf{deg}\,(F(S)) \geq n-k\}, \\ \mathsf{D}_F(k) &= n - \mathsf{max}\{\mathsf{deg}\,(F(S)) \;:\; \mathsf{deg}\,(S) \leq n-k\}, \end{aligned}$$

where $S \in \mathcal{P}(\mathbb{F}_q)$ *denotes the powerset of* $\mathbb{F}_q$.

Proof. Assume $n - t = \mathsf{max}\{\mathsf{deg}\,(F(S)) \;:\; \mathsf{deg}\,(S) \leq n-k\}$ and S' be such an S. We have by (4)

$$\sum_{x \in F(S')} x^j \begin{cases} = 0 & \text{if } \mathsf{wt}(j) < t \\ \neq 0 & \text{for some } j \text{ with } \mathsf{wt}(j) = t \end{cases}$$

if and only if

$$\sum_{x \in S'} F(x)^j \begin{cases} = 0 & \text{if } \mathsf{wt}(j) < t \\ \neq 0 & \text{for some } j \text{ with } \mathsf{wt}(j) = t \end{cases}$$

if and only if

$$\sum_{x \in \mathbb{F}_q} (\chi_{S'} \cdot F^j)(x) \begin{cases} = 0 & \text{if } \mathsf{wt}(j) < t \\ \neq 0 & \text{for some } j \text{ with } \mathsf{wt}(j) = t \end{cases}$$

But this means $t = \mathsf{min}\{\mathsf{wt}(j) \;:\; \mathsf{deg}\left(F^j\right) \geq k\}$.

Similarly, assume $n-t = \mathsf{min}\{\mathsf{deg}\,(S) \;:\; \mathsf{deg}\,(F(S)) \geq n-k\}$ and S' be such an S. We have by (4)

$$\sum_{x\in F(S')} x^d \begin{cases} \neq 0 & \text{for some } d=j \text{ with } \mathsf{wt}(j) \leq k \\ =0 & \text{if } \mathsf{wt}(d) < \mathsf{wt}(j) \end{cases}$$

if and only if

$$\sum_{x\in S'} F(x)^d \begin{cases} \neq 0 & \text{for some } d=j \text{ with } \mathsf{wt}(j) \leq k \\ =0 & \text{if } \mathsf{wt}(d) < \mathsf{wt}(j) \end{cases}$$

if and only if

$$\sum_{x\in \mathbb{F}_q} (\chi_{S'} \cdot F^d)(x) \begin{cases} \neq 0 & \text{for some } d=j \text{ with } \mathsf{wt}(j) \leq k \\ =0 & \text{if } \mathsf{wt}(d) < \mathsf{wt}(j) \end{cases}$$

But this means $t = \mathsf{max}\{\mathsf{deg}\left(F^j\right) \;:\; \mathsf{wt}(j) \leq k\}$, since $\mathsf{deg}\,(S') + \mathsf{deg}\left(F^d\right) = n$. □ □

The characteristic $\mathsf{C}_F(k)$ is related to the following extension of the degree of a function.

Definition 11 (Degree of t-products)**.** Let $F : \mathbb{F}_q \to \mathbb{F}_q$ be a function, and F_i be its Boolean components. For any integer $1 \leq t \leq n$

$$\delta_k(F) = \mathsf{max}_{I\in\mathcal{P}_k^n} \left\{ \mathsf{deg}\left(\prod_{i\in I} F_i \right) \right\}$$

Corollary 12 (to Theorem 8)**.** *We have*

$$\mathsf{C}_F(k) = \delta_k(F).$$

Proof. Theorem 8 shows $\mathsf{C}_F(k) = \mathsf{max}_{\mathsf{wt}(u)\leq k} \{\mathsf{deg}\,(\pi_u \circ F)\}$. It is clear that the right hand side is equivalent to $\delta_k(F)$. □

Remark 13. The characteristic $\mathsf{D}_F(k)$ is equivalent to the characteristic

$$\mathsf{D'}_F(k) = \mathsf{min}\{\mathsf{deg}\,(G) \;:\; \mathsf{deg}\,(G\circ F) \geq k\},$$

and it is much easier to compute. Similarly the characteristic $\mathsf{D}_F(k)$ is equivalent to

$$\mathsf{C'}_F(k) = \mathsf{max}\{\mathsf{deg}\,(G\circ F) \;:\; \mathsf{deg}\,(G) \leq k\}.$$

We will now prove the duality between $\mathsf{C}_F(k)$ and $\mathsf{D}_{F^{\mathsf{inv}}}(n-k)$ for a permutation F.

Theorem 14. *The* $\mathsf{C}_F(k)$ *and* $\mathsf{D}_{F^{\mathsf{inv}}}(n-k)$ *satisfy*

$$\mathsf{C}_F(k) + \mathsf{D}_{F^{\mathsf{inv}}}(n-k) = n.$$

Proof. Recall

$$\begin{aligned}\mathsf{C}_F(k) &= \mathsf{max}\{\mathsf{deg}\,(F^e)\ :\ \mathsf{wt}(e) \leq k\},\\ \mathsf{D}_{F^{\mathsf{inv}}}(n-k) &= \mathsf{min}\{\mathsf{wt}(d)\ :\ \mathsf{deg}\left((F^{\mathsf{inv}})^d\right) \geq n-k\}.\end{aligned}$$

Let $\mathsf{D}_{F^{\mathsf{inv}}}(n-k) = t$. We have a minimum weight d satisfying $\mathsf{wt}(d) = t$ and there exists an i with $\mathsf{wt}(i) \geq n-k$ such that

$$-\sum_{x\in\mathbb{F}_q^*}(F^{\mathsf{inv}}(x))^d x^{-i} \neq 0,$$

using the DFT. Employing $x = F(y)$ we get

$$-\sum_{y\in\mathbb{F}_q^*}(F(y))^{-i} x^d \neq 0.$$

This means $\mathsf{deg}\left(F^{-i}\right) \geq \mathsf{wt}(-d) = n-t$. Since $\mathsf{wt}(-i) \leq k$ we have $\mathsf{C}_F(k) \geq n-t$. So

$$\mathsf{C}_F(k) + \mathsf{D}_{F^{\mathsf{inv}}}(n-k) \geq n.$$

Conversely, let $\mathsf{C}_F(k) = u$, which is satisfied by $u = \mathsf{deg}\,(F^e)$. Then, there exists an i with $\mathsf{wt}(i) = u$ such that

$$-\sum_{x\in\mathbb{F}_q^*}(F(x))^e x^{-i} \neq 0,$$

using the DFT. Employing $x = F(y)$ we get

$$-\sum_{y\in\mathbb{F}_q^*}(F^{\mathsf{inv}}(y))^{-i} x^e \neq 0.$$

This means $\mathsf{deg}\left((F^{\mathsf{inv}}(x))^{-i}\right) \geq \mathsf{wt}(-e) \geq n-k$ and $\mathsf{wt}(-i) = n-u$. Hence $\mathsf{D}_{F^{\mathsf{inv}}}(n-k) \leq n-u$ and

$$\mathsf{C}_F(k) + \mathsf{D}_{F^{\mathsf{inv}}}(n-k) \leq n.$$

The two inequalities give us the result we need. □ □

In the next theorem we note the optimal values for the two characteristics.

Theorem 15. *Let $F : \mathbb{F}_q \to \mathbb{F}_q$ be a permutation which satisfies $\mathsf{deg}\,(F) = d$. The optimal values for the characteristics are*

$$\begin{aligned}\mathsf{C}_F(k) &= \mathsf{min}(kd, n-1),\\ \mathsf{D}_F(k) &= \left\lceil \frac{k}{d} \right\rceil,\end{aligned}$$

for $1 \leq k \leq n-1$.

3.1 Some consequences

The DFT method we explore in this paper is quite useful as exemplified by re-proving the following very interesting theorem of Boura and Canteaut.

Theorem 16 ([6, Theorem 3.1]). *Let $F : \mathbb{F}_q \to \mathbb{F}_q$ be a permutation. Then for any integers k, l*

$$\delta_k(F^{\mathsf{inv}}) < n - k \iff \delta_l(F) < n - l$$

Proof. Using DFT

$$\delta_k(F^{\mathsf{inv}}) < n - k \iff -\sum_{x \in \mathbb{F}_q} (F^{\mathsf{inv}}(x))^d x^{-i} = 0$$

for all d, i with $\mathsf{wt}(d) \leq k$ and $\mathsf{wt}(i) \geq n - l$. Using $x = F(y)$ we get

$$\iff -\sum_{y \in \mathbb{F}_q} (F(y))^{-i} y^d = 0 \iff \delta_l(F) < n - l$$

since $\mathsf{wt}(-i) \leq l$ and $\mathsf{wt}(-d) \geq n - k$ and using DFT once again. □

Remark 17. One can prove Theorem 14 using Theorem 16 as well [14].

In [18], the authors prove several properties of the sets satisfying the division property. With the DFT approach we can reprove these results quite naturally.

Theorem 18 ([18, Theorem 1]). *Let $S \subseteq \mathbb{F}_q$ satisfy division property $\mathcal{D}_k^n$. Then $\#S \geq 2^k$.*

Proof. We have by Corollary 9 $\mathsf{deg}\,(S) = d \leq n - k$. Let $\chi_S = x_1 x_2 \cdots x_d + g$. Then the restriction of χ_S to any 2^{n-d} evaluation $(x_{d+1}, \ldots, x_n) = (\epsilon_{d+1}, \ldots, \epsilon_n)$ where $\epsilon_i \in \mathbb{F}_2$ is maximal degree, i.e., $\sum_{x_1,\ldots,x_d} \chi_S(x_1, \ldots, x_d, \epsilon_{d+1}, \ldots, \epsilon_n)$ is odd. Therefore the weight of $\chi_S = \#S \geq 2^{n-d} \geq 2^k$. □ □

Theorem 19 ([18, Corollary 1]). *Let $\emptyset \neq S \subseteq \mathbb{F}_q$ satisfy division property $\mathcal{D}_n^n$. Then $S = \mathbb{F}_q$.*

Proof. This means $\chi_S = 1$, i.e., $S = \mathbb{F}_q$. □ □

Similar results can be proved rather directly using the DFT approach taken here. For instance the BALANCE property [9] which states that the sum of all elements in S is 0, is clearly equivalent to $\mathsf{deg}\,(S) \leq n - 2$.

3.2 Affine Equivalence of the characteristics

Two functions $F, G : \mathbb{F}_q \to \mathbb{F}_q$ are said to be affinely equivalent if there exists two affine permutations L_1, L_2 such that $G = L_1 \circ F \circ L_2$.

Theorem 20. *The characteristics $\mathsf{C}_F(k)$ and $\mathsf{D}_F(k)$ are invariant under affine equivalence.*

Proof. We will show, using the interpretation of Theorem 10, that the characteristics $\mathsf{C}_F(k)$ and $\mathsf{D}_F(k)$ are the same as that of $G = L_1 \circ F \circ L_2$ as well. First, for a linear permutation L

$$L(S) = \{L(x) \ : \ x \in S\}$$

a degree k set S is mapped to $L(S)$. By Theorem 8 we need to find weights of i for which

$$\sum_{x \in S} L(x)^i = 0$$

is satisfied. We have

$$-\sum_{x \in S} L(x)^{-i} = -\sum_{x \in \mathbb{F}_q} \chi_S(x) L(x)^{-i} = -\sum_{x \in \mathbb{F}_q} \chi_S \circ L^{\mathsf{inv}}(x) x^{-i}$$

Since the degrees of a Boolean function f and $f \circ L$ are the same we prove the claim by the properties of the DFT. □ □

Remark 21. The characteristics are not CCZ-invariant. This is immediate to see when x^d and its inverse $x^{d^{-1}}$ have different degrees. They are not even extended-affine invariant, i.e., $G = L_1 \circ F \circ L_2 + L_3$, where L_1, L_2 are affine permutations and L_3 an affine function.

4 Division Properties of the S-boxes in CAESAR Candidates

Authenticated encryption schemes that aim to provide both privacy and integrity of data, have gained renewed attention in light of the CAESAR competition [2]. In this section we will provide information on their behavior under the characteristics $\mathsf{C}_n(k)$ and $\mathsf{D}_n(k)$.

There are 29 second-round candidates out of the 57 first-round submissions. A significant fraction of the candidates are using SPN as the primitives, around half of them are using AES. Nevertheless there are designs based on new SPN primitives. According to the size of the S-box which is using, we classify them as follows:

4-bit S-boxes: CLOC [12], SILC [13] use the PRESENT [5] S-box. Minalpher [17] uses its own 4-bit S-box. Both S-boxes have the same division properties. They are listed in Table 1.

5-bit S-boxes: Ketje [4], Keyak [3] and Ascon [10] use 5-bit S-boxes with degree 2. The S-box of ICEPOLE [15] has degree 4. The S-box of PRIMATEs [1] has degree 3. The division properties of these S-boxes are described in Table 2.

8-bit S-box: SCREAM [11] constructs an 8-bit S-box from a 4-bit S-box by using the MISTY structure, while STRIBOB [16] employs its own 8-bit S-box. The division properties of these S-boxes are shown in Table 3.

The results in Table 1–Table 3 indicate that none of the candidates in Round 2 of the CAESAR competition uses S-boxes that are vulnerable against attacks using the division property: their $\mathsf{D}_F(k)$ values are optimal according to Theorem 15.

Table 1: Division Properties of the S-boxes used in CLOC, SILC and Minalpher

k	0	1	2	3	4
D_k^4	0	1	1	1	4

Table 2: Division Properties of the S-boxes used in Ketje, Keyak, Ascon and PRIMATEs (D_k^5a) and of the S-boxes used in ICEPOLE (D_k^5b)

k	0	1	2	3	4	5
D_k^5a	0	1	1	2	2	5
D_k^5b	0	1	1	1	1	5

Table 3: Division Properties of the S-boxes used in SCREAM and STRIBOB

k	0	1	2	3	4	5	6	7	8
D_k^8	0	1	1	1	1	1	1	1	8

5 Conclusion

In this paper we showed that the division property is equivalent to a very natural concept used in finite fields: the degree. The discrete Fourier transform, DFT, is a strong tool and allows proving results related to the division property in a natural way. We have made this relationship clear which, we hope, will help analysis of crypanalytical implications. We have also evaluated the resistance of candidate ciphers in the CAESAR competition against the division property.

Acknowledgments

This work was supported by the Research Fund KU Leuven, OT/13/071. Qingju Wang is in part supported by the National Natural Science Foundation of China (no. 61472250), Major State Basic Research Development Program (973 Plan, no. 2013CB338004).

References

[1] E. Andreeva, B. Bilgin, A. Bogdanov, A. Luykx, F. Mendel, B. Mennink, N. Mouha, Q. Wang, and K. Yasuda, *PRIMATEs v1 (2014)*.

[2] D. Bernstein, *CAESAR: Competition for authenticated encryption: Security, applicability, and robustness*, 2014.

[3] G. Bertoni, J. Daemen, M. Peeters, G. Assche, and R. Keer, *Caesar submission: Keyak v1 (2014)*, Submission to the CAESAR competition.

[4] ——, *Caesar submission: Ketje v1 (2014)*, Submission to the CAESAR competition, (2014).

[5] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, *PRESENT: an ultra-lightweight block cipher*, in Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings, P. Paillier and I. Verbauwhede, eds., vol. 4727 of Lecture Notes in Computer Science, Springer, 2007, pp. 450–466.

[6] C. Boura and A. Canteaut, *On the influence of the algebraic degree of f^{-1} on the algebraic degree of $G \circ F$*, IEEE Transactions on Information Theory, 59 (2013), pp. 691–702.

[7] A. Canteaut and M. Videau, *Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis*, in Advances in cryptology—EUROCRYPT 2002 (Amsterdam), vol. 2332 of Lecture Notes in Comput. Sci., Springer, Berlin, 2002, pp. 518–533.

[8] C. Carlet, *Vectorial Boolean functions for cryptography.* Manuscript, to appear as a chapter of *Boolean Methods and Models*, Cambridge University Press, 2006.

[9] J. Daemen, L. R. Knudsen, and V. Rijmen, *The block cipher Square*, in Fast Software Encryption, 4th International Workshop, FSE '97, Haifa, Israel, January 20-22, 1997, Proceedings, E. Biham, ed., vol. 1267 of Lecture Notes in Computer Science, Springer, 1997, pp. 149–165.

[10] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, *Ascon v1 (2014)*, Submission to the CAESAR competition.

[11] V. Grosso, G. Leurent, F. Standaert, K. Varici, F. Durvaux, L. Gaspar, S. Kerckhof, and E. Inria, *SCREAM & iSCREAM Side-Channel Resistant Authenticated Encryption with Masking*, Submission to the CAESAR competition.

[12] T. Iwata, K. Minematsu, J. Guo, and S. Morioka, *CLOC: Compact low-overhead CFB*, Submission to the CAESAR competition, (2014).

[13] T. Iwata, K. Minematsu, J. Guo, S. Morioka, and E. Kobayashi, *SILC: SImple Lightweight CFB*, Submission to the CAESAR competition, (2014).

[14] W. Meier. personal communication.

[15] P. Morawiecki, K. Gaj, E. Homsirikamol, K. Matusiewicz, J. Pieprzyk, M. Rogawski, M. Srebrny, and M. Wójcik, *ICEPOLE: high-speed, hardware-oriented authenticated encryption*, in Cryptographic Hardware and Embedded Systems–CHES 2014, Springer Berlin Heidelberg, 2014, pp. 392–413.

[16] M.-J. O. Saarinen, *The STRIBOBr1 authenticated encryption algorithm*, Submission to the CAESAR competition.

[17] Y. Sasaki, Y. Todo, K. Aoki, Y. Naito, T. Sugawara, Y. Murakami, M. Matsui, and S. Hirose, *Minalpher v1 (2014)*.

[18] B. Sun, X. Hai, W. Zhang, L. Cheng, and Z. Yang, *New observation on division property*. Cryptology ePrint Archive, Report 2015/459, 2015.

[19] Y. Todo, *Integral cryptanalysis on full MISTY1*, in Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I, R. Gennaro and M. Robshaw, eds., vol. 9215 of Lecture Notes in Computer Science, Springer, 2015, pp. 413–432.

[20] ——, *Structural evaluation by generalized integral property*, in Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I, E. Oswald and M. Fischlin, eds., vol. 9056 of Lecture Notes in Computer Science, Springer, 2015, pp. 287–314.