Relating Undisturbed Bits to Other Properties of Substitution Boxes[⋆]

Rusydi H. Makarim[1] and Cihangir Tezcan[1,2⋆⋆]

[1] Institute of Applied Mathematics
[2] Department of Mathematics
Middle East Technical University, 06800, Çankaya, Ankara, Turkey
{rusydi.makarim, cihangir}@metu.edu.tr

Abstract. Recently it was observed that for a particular nonzero input difference to an S-Box, some bits in all the corresponding output differences may remain invariant. These specific invariant bits are called *undisturbed bits*. Undisturbed bits can also be seen as truncated differentials with probability 1 for an S-Box. The existence of undisturbed bits was found in the S-Box of Present and its inverse. A 13-round improbable differential attack on Present was provided by Tezcan and without using the undisturbed bits in the S-Box an attack of this type can only reach 7 rounds. Although the observation and the cryptanalytic application of undisturbed bits are given, their relation with other properties of an S-Box remain unknown. This paper presents some results on mathematical properties of S-Boxes having undisturbed bits. We show that an S-Box has undisturbed bits if any of its coordinate functions has a nontrivial linear structure. The relation of undisturbed bits with other cryptanalytic tools such as difference distribution table (DDT) and linear approximation table (LAT) are also given. We show that autocorrelation table is proven to be a more useful tool, compared to DDT, to obtain all nonzero input differences that yield undisturbed bits. Autocorrelation table can then be viewed as a counterpart of DDT for truncated differential cryptanalysis. Given an $n \times m$ balanced S-Box, we state that the S-Box has undisturbed bits whenever the degree of any of its coordinate function is quadratic.

Keywords: block cipher, substitution box, undisturbed bits, truncated differential

1 Introduction

The emerging trends of small-scale computing devices raise the need for suitable cryptographic primitives, especially block ciphers. Two main challenges to design

[⋆⋆] The work of the second author was supported by The Scientific and Technological Research Council of Turkey (TÜBİTAK) under the grant 112E101 titled ”Improbable Differential Cryptanalysis of Block Ciphers”.

a block cipher for small-scale devices are the limited memory and available power. Some of the proposals for lightweight block ciphers, such as Present [2] and Rectangle [17], are designed in bit-oriented fashion. This is due to the efficiency of bit-level operation in hardware implementation.

In [16], Tezcan observed that for a particular nonzero input difference to the substitution box (S-Box) of Present, in all of the output differences, there exist some bits that remain the same. These specific invariant bits are called *undisturbed bits*. For instance, with input difference $\mathbf{9} = (1, 0, 0, 1)$ the least significant bit of every possible output difference is undisturbed and its value is equal to zero. The existence of undisturbed bits can also be equally seen as a truncated differential [7] with probability one for a given S-Box. This allows an attacker to have longer truncated differential for bit-oriented ciphers. In [16], a 13-round improbable differential attack was provided for Present and without using undisturbed bits, the best attack of this type can only reach 7 rounds.

Table 1. The 4 × 4 S-Box of Present.

$\overline{x}$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
$S(\overline{x})$	**12**	**5**	**6**	**11**	**9**	**0**	**10**	**13**	**3**	**14**	**15**	**8**	**4**	**7**	**1**	**2**

Proving the exact security bound of a block cipher against differential cryptanalysis is a challenging task. Typically the designer of block cipher would perform computer-aided search to find the best differential characteristic on reduced-round version of the cipher. One obvious way to improve the complexity of the searching algorithm is by reducing the search space. In [15] Sun *et al.* used the undisturbed bits in the S-Box of Present as additional constraint for searching the best differential in related-key settings. The existence of undisturbed bits remove some differential patterns that would never occur and, hence, reduce the search space of the differential characteristics. The undisturbed bits are then converted into linear inequalities for Mixed-Integer Linear Programming (MILP) model. The term *conditional differential propagation* is used by the authors to describe this behaviour.

In [16], it was shown that all 3×3 bijective S-Boxes contain undisturbed bits. Moreover, many 4×4 S-Boxes of cryptographic algorithms are also evaluated in [16], and it was observed that 66% of these S-Boxes contain undisturbed bits. Since bit-oriented lightweight block ciphers use small S-Boxes, undisturbed bits pose a threat to the security of these ciphers.

Although previous literature have discussed the observation on undisturbed bits and its application in cryptanalysis of block ciphers, the relation of undisturbed bits with other properties of an S-Box remain unknown. The main goal of this paper is to address this open problem and presents the relation of undisturbed bits to other properties in an S-Box. All necessary notations and preliminaries on Boolean functions and S-Boxes are given in Sect. 2.

We breakdown the primary goal of this paper into several sub-problems. The first sub-problem is, one may ask the implication of undisturbed bits to the component functions of an S-Box. Specifically, we would like to focus on the component functions of an S-Box where the undisturbed bits occur. The second sub-problem is the relation of undisturbed bits with other cryptanalytic tools for S-Boxes. We want to see the existence of undisturbed bits from the point of view of two well-known cryptanalytic tools, *difference distribution table* (DDT) [1] and *linear approximation table* (LAT) [10]. We will address these two sub-problems and show the relation of undisturbed bits with the notion of linear structure in Sect. 3. The third sub-problem in this work deals with a problem of developing dedicated cryptanalytic tool to obtain all nonzero input differences that yield undisturbed bits. In Sect. 4 autocorrelation table will be introduced as a cryptanalytic tool, in addition to DDT and LAT, that can be used to find undisturbed bits. Lastly, we ask what would be the property of an S-Box that may indicate whether an S-Box has undisturbed bits. We will show in Sect. 5 that a balanced $n \times m$ S-Box with a quadratic coordinate function has undisturbed bits. We conclude this paper in Sect. 6.

2 Notations and Preliminaries

The cardinality of a set V is denoted by $|V|$. Let $\mathbb{F}_2 = \{0, 1\}$ be a finite field with two elements and $\mathbb{F}_2^n$ be n-dimensional vector space over $\mathbb{F}_2$. Any element of $\mathbb{F}_2^n$ is denoted by $\overline{x} = (x_{n-1}, \dots, x_0)$. The notation $\oplus$ is used to denote the addition in $\mathbb{F}_2$ as well as $\mathbb{F}_2^n$. The vector $\overline{x} = (x_{n-1}, \dots, x_0) \in \mathbb{F}_2^n$ can be represented as integer by $\boldsymbol{x} = \sum_{i=0}^{n-1} x_i 2^i$ and its associated integer representation is written using boldface type font. The standard basis for $\mathbb{F}_2^n$ is represented by

$$\overline{e}_{n-1} = (1, 0, 0, \dots, 0), \quad \dots \quad \overline{e}_1 = (0, \dots, 0, 1, 0), \quad \overline{e}_0 = (0, 0, \dots, 0, 1)$$

The vector $\overline{e}_i$ is called the i-th *standard basis* of $\mathbb{F}_2^n$. The integer representation of each i-th standard basis of $\mathbb{F}_2^n$ is given by $\mathbf{2}^i$. The *inner product* of vectors $\overline{x}, \overline{y} \in \mathbb{F}_2^n$ is defined as $\overline{x} \cdot \overline{y} = x_{n-1}y_{n-1} \oplus \dots \oplus x_0 y_0$. The *weight* of vector $\overline{x} \in \mathbb{F}_2^n$ is defined as the number of its nonzero components, denoted $\mathrm{wt}(\overline{x})$. Note that in this paper every vector is considered as column vector, but we will continue writing it in row-wise manner.

2.1 Boolean Functions

A *Boolean function* $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ is a map from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The associated *sign function* $\widehat{f}(\overline{x})$ for every Boolean function f is defined by $\widehat{f}(\overline{x}) = (-1)^{f(\overline{x})} \in \{-1, 1\}$. The *weight* of a Boolean function f, denoted by $\mathrm{wt}(f)$, is defined as $\mathrm{wt}(f) = |\{\overline{x} \in \mathbb{F}_2^n \mid f(\overline{x}) \neq 0\}|$. A Boolean function f with $\mathrm{wt}(f) = 2^{n-1}$ is called a *balanced function.* If for every $\overline{x} \in \mathbb{F}_2^n$ the Boolean function $f(\overline{x}) = \tau$ for a fixed $\tau \in \mathbb{F}_2$, then we call f a *constant function.* The *distance* of two Boolean functions f, g, denoted by $\mathrm{dt}(f, g)$ is defined as the number of entry in which they differ, i.e. $\mathrm{dt}(f, g) = |\{\overline{x} \in \mathbb{F}_2^n \mid f(\overline{x}) \neq g(\overline{x})\}|$.

A Boolean function can be represented using algebraic expression

$$f(\overline{x}) = f(x_{n-1}, \dots, x_1, x_0) = \bigoplus_{\overline{u} \in \mathbb{F}_2^n} a_{\overline{u}} x_{n-1}^{u_{n-1}} \cdots x_0^{u_0} = \bigoplus_{\overline{u} \in \mathbb{F}_2^n} a_{\overline{u}} \overline{x}^{\overline{u}} \qquad (1)$$

The coefficient $a_{\overline{u}}$ is obtained by $a_{\overline{u}} = \bigoplus_{\overline{x} \preceq \overline{u}} f(\overline{x})$ where $\overline{x} \preceq \overline{u}$ means that $x_i \leq u_i$ for all $0 \leq i \leq n-1$ (we say that $\overline{u}$ *covers* $\overline{x}$). We refer to expression given in Equation (1) as the *algebraic normal form* (ANF) of f. The *degree* of Boolean function, $\deg(f)$, is defined as the maximal monomial degree in its ANF representation. The following proposition gives an upper bound of the degree for balanced function.

Proposition 1 ([14]). *For a balanced n-variable Boolean function with $n \geq 2$, $\deg(f) \leq n-1$.*

An *affine function* is a Boolean function such that its ANF is of the form $\overline{\omega} \cdot \overline{x} \oplus \epsilon = \omega_{n-1} x_{n-1} \oplus \cdots \oplus \omega_0 x_0 \oplus \epsilon$ for $\overline{\omega} = (\omega_{n-1}, \dots, \omega_0) \in \mathbb{F}_2^n$ and $\epsilon \in \mathbb{F}_2$. The vector $\overline{\omega}$ is the *coefficient vector* of the affine function. If $\epsilon = 0$, the function $\overline{\omega} \cdot \overline{x}$ is called a *linear function.* The following proposition characterizes the weight of affine functions.

Proposition 2. *Every affine function with nonzero coefficient vector is balanced. If the coefficient vector is zero vector, the affine function is a constant function.*

In the analysis of a Boolean function, *Walsh-Hadamard Transform* is an important tool that could determine various properties of the function. We give the following definition of Walsh-Hadamard Transform as well as its inverse transform.

Definition 1 (Walsh-Hadamard Transform). *The Walsh value of f at $\overline{\omega} \in \mathbb{F}_2^n$ is defined by*

$$\mathcal{W}_f(\overline{\omega}) = \sum_{\overline{x} \in \mathbb{F}_2^n} (-1)^{f(\overline{x})} (-1)^{\overline{\omega} \cdot \overline{x}} = \sum_{\overline{x} \in \mathbb{F}_2^n} \widehat{f}(\overline{x}) (-1)^{\overline{\omega} \cdot \overline{x}}$$

The inverse transform is defined by

$$\widehat{f}(\overline{x}) = 2^{-n} \sum_{\overline{\omega} \in \mathbb{F}_2^n} \mathcal{W}_f(\overline{\omega}) (-1)^{\overline{x} \cdot \overline{\omega}}$$

The vector $(\mathcal{W}_f(\mathbf{0}), \dots, \mathcal{W}_f(\mathbf{2^n - 1}))$ is called the *Walsh spectrum* of f. One of the properties of a Boolean function that can be determined from the Walsh value is balancedness.

Proposition 3. *The Boolean function f is balanced if and only if $\mathcal{W}_f(\overline{0}) = 0$.*

Another important tool in analysis of Boolean functions is the notion of *autocorrelation* and its relation with undisturbed bits are discussed in Sect. 3.

Definition 2 (Autocorrelation). *The autocorrelation of n-variable Boolean function f at $\overline{\alpha} \in \mathbb{F}_2^n$ is defined by*

$$r_f(\overline{\alpha}) = \sum_{\overline{x} \in \mathbb{F}_2^n} (-1)^{f(\overline{x})}(-1)^{f(\overline{x}\oplus\overline{\alpha})} = \sum_{\overline{x} \in \mathbb{F}_2^n} (-1)^{f(\overline{x})\oplus f(\overline{x}\oplus\overline{\alpha})}$$

.

We refer to vector $(r_f(\mathbf{0}), \ldots, r_f(\mathbf{2}^n{-}\mathbf{1}))$ as the *autocorrelation spectrum* of f. The relation of autocorrelation and Walsh-transform is given by the Wiener-Khinthcine's Theorem.

Theorem 1 (Wiener-Khinthcine [12]). *The expression of the autocorrelation in terms of Walsh value is equal to*

$$r_f(\overline{\alpha}) = 2^{-n} \sum_{\overline{\omega} \in \mathbb{F}_2^n} \mathcal{W}_f^2(\overline{\omega})(-1)^{\overline{\alpha}\cdot\overline{\omega}}$$

A cryptographic criteria which is closely related to its autocorrelation is *Strict Avalanche Criterion* (SAC). An n-variable Boolean function f satisfies SAC if changing any one of the n bits in the input results in the output of the function being changed with probability 1/2. It is clear that the following proposition follows from the definition of SAC and could be treated as an equivalent definition.

Proposition 4. *An n-variable Boolean function f satisfies SAC if and only if the function $f(\overline{x}) \oplus f(\overline{x} \oplus \overline{\alpha})$ is balanced for every $\overline{\alpha} \in \mathbb{F}_2^n$ with $wt(\overline{\alpha}) = 1$. Equivalently, the function f satisfies SAC if and only if $r_f(\overline{\alpha}) = 0$, with $wt(\overline{\alpha}) = 1$.*

An n-variable Boolean function is said to satisfy *propagation criterion* of degree k, which we denote by PC(k), if changing any i ($1 \leq i \leq k$) of the n bits in the input results in the output of the function being changed for half of the times. This definition generalizes the notion of SAC, which clearly equals to PC(1) function. The following proposition is analogous to the one given in Proposition 4.

Proposition 5. *An n-variable Boolean function f satisfies PC(k) if and only if all of the given values*

$$r_f(\overline{\alpha}) = \sum_{\overline{x} \in \mathbb{F}_2^n} (-1)^{f(\overline{x})}(-1)^{f(\overline{x}\oplus\overline{\alpha})} = 0 \qquad 1 \leq wt(\overline{\alpha}) \leq k$$

The *derivative* of f at $\overline{\alpha} \in \mathbb{F}_2^n$ is defined as $D_{\overline{\alpha}}f(\overline{x}) = f(\overline{x}) \oplus f(\overline{x} \oplus \overline{\alpha})$. The derivative of f at any point in $\mathbb{F}_2^n$ can also be treated as an n-variable Boolean function. The autocorrelation of a Boolean function can then be expressed in terms of its derivative as $r_f(\overline{\alpha}) = \sum_{\overline{x} \in \mathbb{F}_2^n} (-1)^{D_{\overline{\alpha}}f(\overline{x})}$. The following proposition gives an upper bound of the degree of a derivative function.

Proposition 6 ([9]). *If f is an n-variable Boolean function and $\overline{\alpha} \in \mathbb{F}_2^n$, then* $\deg(D_{\overline{\alpha}}f) \leq \deg(f) - 1$.

If $D_{\overline{\alpha}} f(\overline{x})$ is a constant function, then $\overline{\alpha}$ is a *linear structure* of f [8][6]. The zero vector $\overline{0}$ is a trivial linear structure since $D_{\overline{0}} f(\overline{x}) = 0$ for all $\overline{x} \in \mathbb{F}$

Definition 3 (S-Box with linear structures [5][6][11]). *An $n \times m$ S-Box S is said to have a linear structure if there exists a nonzero vector $\overline{\alpha} \in \mathbb{F}_2^n$ together with a nonzero vector $\overline{b} \in \mathbb{F}_2^m$ such that $\overline{b} \cdot S(\overline{x}) \oplus \overline{b} \cdot S(\overline{x} \oplus \overline{\alpha})$ takes the same value $c \in \mathbb{F}_2$ for all $\overline{x} \in \mathbb{F}_2^n$.*

Proposition 10. *An $n \times m$ S-Box S is said to have a linear structure if there exists a nonzero vector $\overline{\alpha} \in \mathbb{F}_2^n$ together with a nonzero vector $\overline{b} \in \mathbb{F}_2^m$ such that $r_{\overline{b} \cdot S}(\overline{\alpha}) = \pm 2^n$*

In the cryptanalysis of block ciphers, the two most well-known cryptanalytic tools to analyse properties of an S-Box are DDT and LAT.

Let $\overline{x}, \overline{x}' \in \mathbb{F}_2^n$ be two inputs to the S-Box S and $\overline{y} = S(\overline{x})$, $\overline{y}' = S(\overline{x}')$ be their corresponding outputs. We refer to the difference in the input $\overline{x} \oplus \overline{x}' = \overline{\alpha}$ as the *input difference* to S. Similarly $\overline{y} \oplus \overline{y}' = \overline{\beta}$ is the *output difference* of S correponding to input difference $\overline{\alpha}$. DDT examines how many times a certain output difference of an S-Box occur for a given input difference. The definition of DDT is given as follows.

Definition 4. *For an $n \times m$ S-Box S, the entry in the row $\overline{s} \in \mathbb{F}_2^n$ and column $\overline{t} \in \mathbb{F}_2^m$ (considering their integer representation) of difference distribution table of S is defined by $\mathsf{DDT}(\boldsymbol{s}, \boldsymbol{t}) = |\{\overline{x} \in \mathbb{F}_2^n \mid S(\overline{x}) \oplus S(\overline{x} \oplus \overline{s}) = \overline{t}\}|$.*

The probability of an input difference $\overline{\alpha}$ that yields the output difference $\overline{\beta}$ is then defined by

$$\begin{aligned}\mathbf{Pr}_S[\overline{\alpha} \to \overline{\beta}] &= 2^{-n}|\{\overline{x} \in \mathbb{F}_2^n \mid S(\overline{x}) \oplus S(\overline{x} \oplus \overline{\alpha}) = \overline{\beta}\}| \\ &= 2^{-n} \cdot \mathsf{DDT}(\boldsymbol{\alpha}, \boldsymbol{\beta})\end{aligned}$$

On the other hand, LAT is used to find the best linear approximation for an S-Box involving the parity bits of its input and output. The definition of linear approximation table is given as follows.

Definition 5. *For an $n \times m$ S-Box S, the linear approximation table of S at row $\overline{s} \in \mathbb{F}_2^n$ and column $\overline{t} \in \mathbb{F}_2^m$ (considering their integer representation) is defined as*

$$\mathsf{LAT}(\boldsymbol{s}, \boldsymbol{t}) = |\{\overline{x} \in \mathbb{F}_2^n \mid \overline{s} \cdot \overline{x} = \overline{t} \cdot S(\overline{x})\}| - 2^{n-1}$$

3 Undisturbed Bits and Linear Structures

In this section we recall the definition of undisturbed bits and provide its relations with autocorrelation, derivative, and linear structure of coordinate functions in an S-Box. The notation $S = (h_{m-1}, \ldots, h_0)$ will be used consistently for the rest of the paper to denote the $n \times m$ S-Box $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ with coordinate functions $h_{m-1}, \ldots, h_0$, where $h_i : \mathbb{F}_2^n \mapsto \mathbb{F}_2$.

Definition 6 (Undisturbed Bits). *Let $\overline{\alpha} \in \mathbb{F}_2^n$ be a nonzero input difference to S-Box S and $\Omega_{\overline{\alpha}} = \{\overline{\beta} = (\beta_{m-1}, \ldots, \beta_0) \in \mathbb{F}_2^m \mid \mathbf{Pr}_S[\overline{\alpha} \to \overline{\beta}] > 0\}$ be the* *set of all possible output differences of S corresponding to $\overline{\alpha}$. If $\beta_i = c$ for a fixed $c \in \mathbb{F}_2$ and for all $\overline{\beta} \in \Omega_{\overline{\alpha}}$ with $i \in \{0, \dots, m-1\}$, then the S-Box S has undisturbed bits. In particular, we say that for input difference $\overline{\alpha}$, the i-th bit of the output difference of S is undisturbed (and its value is c).*

Recall that any output of the S-Box as the element of $\mathbb{F}_2^m$ can be computed component-wisely using coordinate functions of an S-Box. If $\mathbf{Pr}_S[\overline{\alpha} \to \overline{\beta}] > 0$, then there exists a $\overline{v} \in \mathbb{F}_2^n$ such that $S(\overline{v}) \oplus S(\overline{v} \oplus \overline{\alpha}) = \overline{\beta}$. It follows that the component of the output difference vectors $\overline{\beta} = (\beta_{m-1}, \dots, \beta_0)$ can be obtained by $\beta_i = h_i(\overline{v}) \oplus h_i(\overline{v} \oplus \overline{\alpha})$. The following result is an implication from this observation.

Theorem 2. *For a nonzero input difference $\overline{\alpha} \in \mathbb{F}_2^n$ and $i \in \{0, \dots, m-1\}$, the i-th bit of the output difference of S is undisturbed if and only if $D_{\overline{\alpha}} h_i(\overline{x}) = h_i(\overline{x}) \oplus h_i(\overline{x} \oplus \overline{\alpha})$ is a constant function.*

Proof. Suppose for an input difference $\overline{\alpha}$ the i-th bit of the output difference of S is undisturbed. Let $\Omega_{\overline{\alpha}} = \{\overline{\beta} = (\beta_{m-1}, \dots, \beta_0) \in \mathbb{F}_2^m \mid \mathbf{Pr}_S[\overline{\alpha} \to \overline{\beta}] > 0\}$ be the set of all possible output differences of S corresponding to $\overline{\alpha}$. Definition 6 tells us that for all $\overline{\beta} = (\beta_{m-1}, \dots, \beta_0) \in \Omega_{\overline{\alpha}}$ the component $\beta_i = c$ for a fixed $c \in \mathbb{F}_2$. Since $\beta_i = h_i(\overline{v}) \oplus h_i(\overline{v} \oplus \overline{\alpha})$ for some $\overline{v} \in \mathbb{F}_2^n$ and because the computation of output differences in $\Omega_{\overline{\alpha}}$ run through all the elements of $\mathbb{F}_2^n$, clearly $D_{\overline{\alpha}} h_i(\overline{x}) = h_i(\overline{x}) \oplus h_i(\overline{x} \oplus \overline{\alpha}) = c$ for all $\overline{x} \in \mathbb{F}_2^n$. Hence $D_{\overline{\alpha}} h_i(\overline{x})$ is a constant function. The converse part of the proof can be done by reversing the previous step. □

The value of undisturbed bits can then be deduced whether the constant function $D_{\overline{\alpha}} h_i(\overline{x})$ is equal to zero or one, for each $\overline{x} \in \mathbb{F}_2^n$. Because $D_{\overline{\alpha}} h_i(\overline{x})$ is a constant function, then the nonzero vector $\overline{\alpha}$ is a linear structure of the coordinate function h_i. Equivalently, since $\overline{\alpha}$ is a nonzero vector, then h_i is a function with linear structure. This result shows that a particular S-Box has undisturbed bits if any of its coordinate functions has a nontrivial linear structure. In order to see if an S-Box has undisturbed bits, it is sufficient to check the derivative of each coordinate function at every nonzero element of $\mathbb{F}_2^n$.

Theorem 2 also relates an S-Box which has undisturbed bits with Definition 3 about an S-Box with linear structures. It shows that an S-Box that has undisturbed bits belongs to special class of S-Boxes with linear structures by only considering the existence of linear structures in its coordinate functions. This can be described by the following proposition, and it can be treated as an equivalent definition for an S-Box that has undisturbed bits.

Proposition 11. *An $n \times m$ S-Box S is said to have an undisturbed bit if there exists a nonzero vector $\overline{\alpha} \in \mathbb{F}_2^n$ together with a nonzero vector $\overline{b} \in \mathbb{F}_2^m$ with $wt(b) = 1$ such that $\overline{b} \cdot S(\overline{x}) \oplus \overline{b} \cdot S(\overline{x} \oplus \overline{\alpha})$ takes the same value $c \in \mathbb{F}_2$ for all $\overline{x} \in \mathbb{F}_2^n$.*

In other words, if an S-Box S has undisturbed bits, then S has a linear structure. However, the converse is not true in general. Thus, Definition 3 can be seen as a generalization of undisturbed bits.

The existence of undisturbed bits in an S-Box may also be used to describe the unsatisfiability of the corresponding coordinate functions against SAC. We state it in the following remark.

Remark 1. Let $\mathcal{I}_i = \{\overline{\alpha} \in \mathbb{F}_2^n,\ \overline{\alpha} \neq \overline{0} \mid h_i(\overline{x}) \oplus h_i(\overline{x} \oplus \overline{\alpha})$ is a constant function$\}$ be the set such that for any $\overline{\alpha} \in \mathcal{I}_i$ the i-th bit of the output difference of S is undisturbed. Equivalently $\mathcal{I}_i$ is the set of all nonzero linear structures of the coordinate function h_i, i.e. $\mathcal{I}_i = \mathcal{LS}_{h_i} \setminus \{\overline{0}\}$. We set

$$d = \min_{\overline{\alpha} \in \mathcal{I}_i} \mathrm{wt}(\overline{\alpha})$$

If $d = 1$, then from Proposition 4 it follows that the coordinate function h_i does not satisfy Strict Avalanche Criterion (SAC). However, this remark can not be generalized for $d > 1$. The reason is because if there exists a d' with $1 \leq d' < d$ such that the coordinate function does not satisfy PC(d') then d is not a proper bound for the unsatisfiability condition.

A trivial lemma can be derived from Theorem 2 to indicate whether an S-Box has undisturbed bits from the autocorrelation of its coordinate functions. We will use the following lemma to show the relation of other cryptanalytic tools with undisturbed bits.

Lemma 1. *For a nonzero input difference $\overline{\alpha} \in \mathbb{F}_2^n$, the i-th bit of the output difference of S is undisturbed if and only if*

$$r_{h_i}(\overline{\alpha}) = \pm 2^n$$

for $i \in \{0, \ldots, m-1\}$.

Proof. Suppose for a nonzero input difference $\overline{\alpha} \in \mathbb{F}_2^n$, the i-th bit of the output difference of S is undisturbed. From Theorem 2 the vector $\overline{\alpha}$ is a linear structure of coordinate function h_i. It follows that from Proposition 7 we have $r_{h_i}(\overline{\alpha}) = \pm 2^n$. The converse can be proven by reversing the previous steps. □

The remaining part of this section describes the relation of some existing cryptanalytic tools with undisturbed bits. In particular, we give the relation of undisturbed bits with two most important cryptanalytic tools for an S-Box, namely DDT and LAT. The following theorem of [18] provides a relation between DDT and the autocorrelation of the component functions of an S-Box.

Theorem 3 ([18]). *The relation between difference distribution table and the autocorrelation of the component functions of S is given by*

$$r_{\overline{j} \cdot S}(\overline{\alpha}) = \sum_{\overline{v} \in \mathbb{F}_2^m} \mathsf{DDT}(\boldsymbol{\alpha}, \boldsymbol{v})(-1)^{\overline{j} \cdot \overline{v}}$$

for $\overline{\alpha} \in \mathbb{F}_2^n$ and $\overline{j} \in \mathbb{F}_2^m$.

Using Lemma 1 the relation of undisturbed bits and DDT can be easily shown in Corollary 1.

Corollary 1 (DDT and Undisturbed Bits). *For a nonzero input difference $\overline{\alpha} \in \mathbb{F}_2^n$, the i-th bit of the output difference of S is undisturbed if and only if*

$$\sum_{\overline{v} \in \mathbb{F}_2^m} \mathsf{DDT}(\boldsymbol{\alpha}, \boldsymbol{v})(-1)^{\overline{e_i} \cdot \overline{v}} = \pm 2^n$$

for $i \in \{0, \ldots, m-1\}$ and $\overline{e}_i$ is the i-th standard basis of $\mathbb{F}_2^m$.

Proof. Suppose for a nonzero input difference $\overline{\alpha} \in \mathbb{F}_2^n$, the i-th bit of the output difference of S is undisturbed. From Lemma 1 we have $r_{h_i}(\overline{\alpha}) = \pm 2^n$. Since $r_{h_i}(\overline{\alpha}) = r_{\overline{e}_i \cdot S}(\overline{\alpha})$ it follows from Theorem 3 that $\sum_{\overline{v} \in \mathbb{F}_2^m} \mathsf{DDT}(\boldsymbol{\alpha}, \boldsymbol{v})(-1)^{\overline{e_i} \cdot \overline{v}} = \pm 2^n$. The converse can be trivially proved by reversing the previous steps. □

Linear approximation table (LAT) is used as a counterpart of DDT in the domain of linear cryptanalysis. Although undisturbed bits are useful in constructing truncated differential for bit-oriented cipher, one may also indicate the existence of undisturbed bits from LAT. We will use a well-known relation of LAT and the Walsh value of component functions of an S-Box in Lemma 2. Together with Theorem 1 (Wiener-Khintchine) and Lemma 1, the relation of LAT and undisturbed bits can be established. The main result is given in Theorem 4.

Lemma 2. *The relation between linear approximation table of S and the Walsh transform of the component functions of S is given by*

$$\mathsf{LAT}(\boldsymbol{a}, \boldsymbol{b}) = \frac{1}{2} \mathcal{W}_{\overline{b} \cdot S}(\overline{a})$$

for $\overline{a} \in \mathbb{F}_2^n$ and $\overline{b} \in \mathbb{F}_2^m$.

Theorem 4 (LAT and Undisturbed Bits). *For a nonzero input difference $\overline{\alpha} \in \mathbb{F}_2^n$, the i-th bit of the output difference of S is undisturbed if and only if*

$$2^{2-n} \sum_{\overline{a} \in \mathbb{F}_2^n} \mathsf{LAT}(\boldsymbol{a}, \mathbf{2}^{\boldsymbol{i}})^2 (-1)^{\overline{\alpha} \cdot \overline{a}} = \pm 2^n$$

for $i \in \{0, \ldots, m-1\}$.

Proof. Firstly, we claim that $2^{2-n} \sum_{\overline{a} \in \mathbb{F}_2^n} \mathsf{LAT}(\boldsymbol{a}, \boldsymbol{b})^2 (-1)^{\overline{\alpha} \cdot \overline{a}} = r_{\overline{b} \cdot S}(\overline{\alpha})$. The proof of the claim is as follows

$$\begin{aligned}
2^{2-n} \sum_{\overline{a} \in \mathbb{F}_2^n} \mathsf{LAT}(\boldsymbol{a}, \boldsymbol{b})^2 (-1)^{\overline{\alpha} \cdot \overline{a}} &= 2^{-n} \sum_{\overline{a} \in \mathbb{F}_2^n} 2^2 \cdot \mathsf{LAT}(\boldsymbol{a}, \boldsymbol{b})^2 (-1)^{\overline{\alpha} \cdot \overline{a}} \\
&= 2^{-n} \sum_{\overline{a} \in \mathbb{F}_2^n} (2 \cdot \mathsf{LAT}(\boldsymbol{a}, \boldsymbol{b}))^2 (-1)^{\overline{\alpha} \cdot \overline{a}} \\
&= 2^{-n} \sum_{\overline{a} \in \mathbb{F}_2^n} \mathcal{W}_{\overline{b} \cdot S}(\overline{a})^2 (-1)^{\overline{\alpha} \cdot \overline{a}} && \text{from Lemma 2} \\
&= r_{\overline{b} \cdot S}(\overline{\alpha}) && \text{from Theorem 1}
\end{aligned}$$

Clearly we have

$$2^{2-n} \sum_{\overline{a} \in \mathbb{F}_2^n} \mathsf{LAT}(\boldsymbol{a}, \boldsymbol{2^i})^2 (-1)^{\overline{\alpha} \cdot \overline{a}} = r_{\overline{e}_i \cdot S}(\overline{\alpha}) = r_{h_i}(\overline{\alpha}) = \pm 2^n$$

where $\overline{e}_i$ is the i-th standard basis of $\mathbb{F}_2^m$. Immediately from Lemma 1, for nonzero input difference $\overline{\alpha}$ the i-th bit of the output difference of S is undisturbed.

Conversely, if for a nonzero input difference $\overline{\alpha}$ the i-th bit of the output difference of S is undisturbed, Lemma 1 implies that $r_{h_i}(\overline{\alpha}) = \pm 2^n$. From our claim we can have $\pm 2^n = r_{\overline{e_i} \cdot S}(\overline{\alpha}) = 2^{2-n} \sum_{\overline{a} \in \mathbb{F}_2^n} \mathsf{LAT}(\boldsymbol{a}, \boldsymbol{2^i})^2 (-1)^{\overline{\alpha} \cdot \overline{a}}$. □

4 Autocorrelation Table

One way to check the existence of undisturbed bits in an S-Box is by taking a nonzero input difference and see whether there are some bits in all the corresponding output differences that remain invariant. This can be done by observing the DDT of an S-Box. However, this indirect approach can be improved if one is able to find a dedicated cryptanalytic tool for the case of undisturbed bits.

In this section, we extend the result of Lemma 1 and provide a tool called *autocorrelation table*, which was also appeared previously in [18]. Though it was introduced earlier, the application of autocorrelation table for cryptanalysis of block ciphers was not mentioned. We will show that autocorrelation table is proven to be a more useful tool, compared to DDT, to check if an S-Box has undisturbed bits. Moreover, we will be able to obtain all nonzero input differences that has undisturbed bits in its corresponding output differences. Because undisturbed bit is also a truncated differential of probability one in an S-Box, autocorrelation table can be viewed as a counterpart of DDT in the domain of truncated differential cryptanalysis.

Definition 7 (Autocorrelation Table [18]). *For $\overline{a} \in \mathbb{F}_2^n$ and $\overline{b} \in \mathbb{F}_2^m$, we define autocorrelation table of S-Box S, denoted as ACT, where the entry in the row $\boldsymbol{a}$ and column $\boldsymbol{b}$ is equal to*

$$\mathsf{ACT}(\boldsymbol{a}, \boldsymbol{b}) = r_{\overline{b} \cdot S}(\overline{a})$$

Proposition 10 provides an equivalent description of an S-Box that has linear structure from the the autocorrelation of its component functions. Autocorrelation table can then be used to determine if an S-Box has linear structure.

Theorem 5. *An S-Box S has a linear structure if and only if there exists a nonzero $\overline{\alpha} \in \mathbb{F}_2^n$ and a nonzero $\overline{b} \in \mathbb{F}_2^m$ such that $\mathsf{ACT}(\boldsymbol{\alpha}, \boldsymbol{b}) = \pm 2^n$.*

Proof. This is an immediate consequences from Definition 3 and Proposition 10. □

Remark 2. Let $\overline{\alpha}$ be an input difference to S and let

$$\Omega_{\overline{\alpha}} = \{\overline{\beta} \in \mathbb{F}_2^m \mid \mathbf{Pr}_S[\overline{\alpha} \to \overline{\beta}] > 0\}$$

be the set of all possible output differences of S corresponding to $\overline{\alpha}$. If the entry $\mathrm{ACT}(\boldsymbol{\alpha}, \boldsymbol{b}) = +2^n$ (resp. -2^n), for $\overline{b} \in \mathbb{F}_2^m$, then $\overline{b} \cdot \overline{\beta} = 0$ (resp. 1) for all $\overline{\beta} \in \Omega_{\overline{\alpha}}$.

To determine if an S-Box has undisturbed bits, it is sufficient to observe nonzero row entries in each column of autocorrelation table that correspond to the autocorrelation spectrum of coordinate functions of the S-Box, i.e. the column $\mathbf{2}^i,\ i \in \{0, \ldots, m-1\}$. The result is given as the following corollary.

Corollary 2. *For a nonzero input difference $\overline{\alpha}$, the i-th bit of the output difference of S is undisturbed if and only if $\mathsf{ACT}(\boldsymbol{\alpha}, \mathbf{2}^i) = \pm 2^n$, for $i \in \{0, \ldots, m-1\}$.*

Proof. From Theorem 2, the vector $\overline{\alpha}$ is a linear structure of the coordinate function h_i. Clearly this is a direct consequence of Theorem 5. □

Autocorrelation table of the S-Box of Present is provided in Table 2. Some input differences that have undisturbed bits in its corresponding output differences can be observed in column **1**, which is the autocorrelation spectrum of the rightmost coordinate function. One may see in row entries **1**, **8**, and **9** at column **1** have value $\pm 2^4 = \pm 16$. Note that the row index represents the input difference and the column index represents the component functions of the S-Box. The magnitude of the entry indicate the value of undisturbed bits, where the sign "+" and "−" correspond to the undisturbed bit value equal to zero and one, respectively.

Table 2. Autocorrelation table of the S-Box of Present. Column **1** correspond to the autocorrelation spectrum of the rightmost coordinate function h_0. Notice that the row entries $\mathbf{1}, \mathbf{8}, \mathbf{9}$ are equal to ± 16. Thus, for input difference $\mathbf{1}, \mathbf{8}, \mathbf{9}$, the 0-th bit of the output difference of Present's S-Box is undisturbed. The value of undisturbed bits is either 0 or 1, depending whether the magnitude is + or −, respectively.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	−16	0	0	0	0	0	0	0	0	−16	16	0	0	0	0
2	16	0	0	−8	−8	0	−8	8	0	−8	0	0	0	0	0	8
3	16	0	−8	0	0	−8	0	0	8	0	0	0	−8	−8	8	0
4	16	0	0	−8	−8	0	0	0	0	−8	0	0	−8	8	0	8
5	16	0	8	0	0	−8	−8	−8	−8	0	0	0	0	0	8	0
6	16	0	−8	8	0	0	0	0	−8	8	0	−16	0	0	0	0
7	16	0	0	0	0	0	8	−8	0	0	0	−16	8	−8	0	0
8	16	−16	−8	8	0	0	0	0	−8	8	0	0	0	0	0	0
9	16	16	0	0	−8	−8	0	0	0	0	0	0	0	0	−8	−8
10	16	0	0	−8	0	8	−8	8	0	−8	0	0	0	0	−8	0
11	16	0	8	0	8	0	0	0	−8	0	0	0	−8	−8	0	−8
12	16	0	0	−8	0	8	0	0	0	−8	0	0	−8	8	−8	0
13	16	0	−8	0	8	0	−8	−8	8	0	0	0	0	0	0	−8
14	16	0	0	0	0	0	0	0	0	0	−16	0	0	0	0	0
15	16	0	0	0	−8	−8	8	−8	0	0	16	0	8	−8	−8	−8

In Table 2 one may also find component functions, other than the coordinate functions, which have linear structures. For instance, the component functions in S-Box of PRESENT represented by $\mathbf{10} \cdot S(\overline{x})$ and $\mathbf{11} \cdot S(\overline{x})$ have nontrivial linear structures (this can be seen in column **10** and **11** in Table 2 where some of the nonzero row entries are equal to $\pm 2^n$). The implication of this result was given in Remark 2. However, it remains unknown whether the existence of linear structures in component functions of an S-Box other than the coordinate functions could improve or lead to a new approach in (truncated)-differential cryptanalysis of bit-oriented block cipher.

5 S-Boxes with Undisturbed Bits

Recall from Theorem 2 that an S-Box has undisturbed bits if the derivative of any of its coordinate function at a nonzero vector in $\mathbb{F}_2^n$ is a constant function. The existence of an S-Box that has undisturbed bits can then be reduced into a question whether any of the coordinate functions of the S-Box has a nonzero linear structure.

So far the known Boolean functions that have nonzero linear structures are affine functions (from Proposition 8). If an S-Box has affine coordinate function, then definitely the S-Box has undisturbed bits. However, this is unlikely to occur in real case. This will lead to a linear approximation that involves input and output bits of the S-Box with probability one, and clearly does not serve its purpose as a nonlinear layer for block ciphers.

In order to find Boolean functions with linear structure, Proposition 6 restrict our attention to the Boolean functions of low degree. The following result is due to Carlet [4]. The complete proof of the following lemma is given in the appendix.

Lemma 3 ([4]). *If f is a balanced n-variable Boolean function with* $\deg(f) = 2$*, then there exists a nonzero $\overline{\alpha} \in \mathbb{F}_2^n$ such that $D_{\overline{\alpha}} f(\overline{x}) = f(\overline{x}) \oplus f(\overline{x} \oplus \overline{\alpha}) = 1$ for all $\overline{x} \in \mathbb{F}_2^n$.*

We extend the result from Lemma 3 in Theorem 6 to show that an S-Box with at least one quadratic coordinate function has undisturbed bits. Hence we show that one may determine whether an S-Box has undisturbed bits from the degree of its coordinate functions.

Theorem 6. *Let S be a balanced $n \times m$ S-Box and $h_{m-1}, \ldots, h_0$ be its coordinate functions. If there exists a coordinate function h_i with* $\deg(h_i) = 2$ *then the S-Box S has undisturbed bits. More precisely, there exists a nonzero $\overline{\alpha} \in \mathbb{F}_2^n$ such that for input difference $\overline{\alpha}$, the i-th bit of the output difference of S is undisturbed and its value is* 1.

Proof. From Proposition 9, for every nonzero $\overline{b} \in \mathbb{F}_2^m$ all the component functions $\overline{b} \cdot S(\overline{x})$ are balanced Boolean functions, including the coordinate functions $h_{m-1}, \ldots, h_0$ of S. If there exists a coordinate function h_i with $\deg(h_i) = 2$, Lemma 3 says that there is a nonzero $\overline{\alpha} \in \mathbb{F}_2^n$ such that $D_{\overline{\alpha}} h_i(\overline{x}) = 1$ for all $\overline{x} \in \mathbb{F}_2^n$. Theorem 2 implies that for input difference $\overline{\alpha}$, the i-th bit of the output difference of S is undisturbed and its value is 1. □

Corollary 3. *If S is a balanced $n \times m$ S-Box with $n = 3$, then S has undisturbed bits. Moreover, for every $i \in \{0, \ldots, m-1\}$ there exists a nonzero $\overline{\alpha} \in \mathbb{F}_2^n$ such that for input difference $\overline{\alpha}$, the i-th bit of the output difference of S is undisturbed and its value is* 1.

Proof. Since S is a balanced S-Box, based on Proposition 1 then $\deg(\overline{b} \cdot S) \leq 2$ for all nonzero $\overline{b} \in \mathbb{F}_2^m$. It follows that every coordinate functions of S is of degree ≤ 2. The results follows immediately from Theorem 6 and Proposition 8. □

In [16] it was stated that every bijective 3×3 S-Box has undisturbed bits. Since bijective 3×3 S-Boxes are balanced S-Boxes, it follows immediately from Corollary 3 that they have undisturbed bits. This can be seen as an alternative proof of [16] where the author used the equivalence classes of 3×3 bijective S-Boxes.

Corollary 4. *Every 3×3 bijective S-Box has undisturbed bits.*

6 Conclusion and Further Remarks

In this work we define the notion of undisturbed bits of an S-Box and give its relation with other properties. S-Boxes which have undisturbed bits are shown to be a special class of S-Boxes with linear structures. We also show that it is possible to indicate whether an S-Box has undisturbed bits or not by using DDT and LAT. Autocorrelation table of an S-Box can be used as a dedicated tool to find nonzero input differences which have undisturbed bits in its output differences. The last result of this paper is the existence of undisturbed bits for balanced $n \times m$ S-Boxes with quadratic coordinate functions.

While the notion of undisturbed bits is related to the existence of nonzero linear structures in the coordinate functions of an S-Box, we also showed that other component functions of an S-Box may have nonzero linear structures. It remains unknown whether this property in an S-Box could improve or lead to a new approach in cryptanalysis of bit-oriented block ciphers.

References

1. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. J. Cryptology 4(1), 3–72 (1991)
2. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES. Lecture Notes in Computer Science, vol. 4727, pp. 450–466. Springer (2007)
3. Carlet, C.: Boolean Models and Methods in Mathematics, Computer Science, and Engineering, chap. Vectorial Boolean Functions for Cryptography, pp. 398–469. Cambridge University Press (2010)
4. Carlet, C.: Boolean Models and Methods in Mathematics, Computer Science, and Engineering, chap. Boolean Functions for Cryptography and Error Correcting Codes, pp. 257–397. Cambridge University Press (2010)

5. Chaum, D., Evertse, J.H.: Crytanalysis of DES with a Reduced Number of Rounds: Sequences of Linear Factors in Block Ciphers. In: Williams, H.C. (ed.) CRYPTO. Lecture Notes in Computer Science, vol. 218, pp. 192–211. Springer (1985)
6. Evertse, J.H.: Linear Structures in Blockciphers. In: Chaum, D., Price, W.L. (eds.) EUROCRYPT. Lecture Notes in Computer Science, vol. 304, pp. 249–266. Springer (1987)
7. Knudsen, L.R.: Truncated and Higher Order Differentials. In: Preneel [13], pp. 196–211
8. Lai, X.: Additive and Linear Structures of Cryptographic Functions. In: Preneel [13], pp. 75–85
9. Lai, X.: Higher order derivatives and differential cryptanalysis. In: Blahut, R., Costello, DanielJ., J., Maurer, U., Mittelholzer, T. (eds.) Communications and Cryptography, The Springer International Series in Engineering and Computer Science, vol. 276, pp. 227–233. Springer US (1994)
10. Matsui, M.: Linear Cryptoanalysis Method for DES Cipher. In: Helleseth, T. (ed.) EUROCRYPT. Lecture Notes in Computer Science, vol. 765, pp. 386–397. Springer (1993)
11. Meier, W., Staffelbach, O.: Nonlinearity Criteria for Cryptographic Functions. In: Quisquater, J.J., Vandewalle, J. (eds.) EUROCRYPT. Lecture Notes in Computer Science, vol. 434, pp. 549–562. Springer (1989)
12. Preneel, B.: Analysis and Design of Cryptographic Hash Functions. Ph.D. thesis, Katholieke Universiteit Leuven (1993), rené Govaerts and Joos Vandewalle (promotors)
13. Preneel, B. (ed.): Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings, Lecture Notes in Computer Science, vol. 1008. Springer (1995)
14. Sarkar, P., Maitra, S.: Construction of Nonlinear Boolean Functions with Important Cryptographic Properties. In: Preneel, B. (ed.) EUROCRYPT. Lecture Notes in Computer Science, vol. 1807, pp. 485–506. Springer (2000)
15. Sun, S., Hu, L., Wang, P.: Automatic Security Evaluation for Bit-oriented Block Ciphers in Related-Key Model : Application to PRESENT-80, LBlock, and Others. IACR Cryptology ePrint Archive 2013, 676 (2013)
16. Tezcan, C.: Improbable Differential Attacks on PRESENT using Undisturbed Bits. Journal of Computational and Applied Mathematics 259, Part B(0), 503 – 511 (2014)
17. Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., Verbauwhede, I.: RECTANGLE: A Bit-slice Ultra-Lightweight Block Cipher Suitable for Multiple Platforms. IACR Cryptology ePrint Archive 2014, 84 (2014)
18. Zhang, X.M., Zheng, Y., Imai, H.: Relating Differential Distribution Tables to Other Properties of Substitution Boxes. Des. Codes Cryptography 19(1), 45–63 (2000)

7 Appendix

7.1 Proof of Lemma 3

Before proving the result in Lemma 3, the following two propositions are required.

Proposition 12 ([4]). *Let f be n-variable Boolean function. We have the following relation*

$$\mathcal{W}_f^2(\overline{0}) = \sum_{\overline{b}\in\mathbb{F}_2^n} \mathcal{W}_{D_{\overline{b}}f}(\overline{0})$$

Proof.

$$\begin{aligned}\sum_{\overline{b}\in\mathbb{F}_2^n} \mathcal{W}_{D_{\overline{b}}f}(\overline{0}) &= \sum_{\overline{b}\in\mathbb{F}_2^n}\left[\sum_{\overline{x}\in\mathbb{F}_2^n}(-1)^{D_{\overline{b}}f(\overline{x})}(-1)^{\overline{0}\cdot\overline{x}}\right] = \sum_{\overline{b}\in\mathbb{F}_2^n}\left[\sum_{\overline{x}\in\mathbb{F}_2^n}(-1)^{D_{\overline{b}}f(\overline{x})}\right]\\ &= \sum_{\overline{b}\in\mathbb{F}_2^n} r_f(\overline{b}) = \sum_{\overline{b}\in\mathbb{F}_2^n} r_f(\overline{b})(-1)^{\overline{0}\cdot\overline{b}} = \mathcal{W}_f^2(\overline{0})\end{aligned}$$

□

Proposition 13 ([4]). *If f is an n-variables Boolean function with* $\deg(f) = 2$ *then*

$$\mathcal{W}_f^2(\overline{0}) = 2^n \sum_{\overline{b}\in\mathcal{LS}_f}(-1)^{D_{\overline{b}}f(\overline{0})}$$

Proof. Since the degree of f is equal to 2, it follows from Proposition 6 that for every $\overline{b} \in \mathbb{F}_2^n$ we have $\deg(D_{\overline{b}}f) \leq 1$. Clearly $D_{\overline{b}}f$ is affine, hence from Proposition 2 it is either balanced (for nonzero coefficient vector) or constant function (for zero coefficient vector). Consequently, for the case where $D_{\overline{b}}f$ is balanced, we have $\mathcal{W}_{D_{\overline{b}}f}(\overline{0}) = 0$ from Proposition 3. Using the result from the Proposition 12, then

$$\begin{aligned}\mathcal{W}_f^2(\overline{0}) &= \sum_{\overline{b}\in\mathbb{F}_2^n} \mathcal{W}_{D_{\overline{b}}f}(\overline{0}) = \sum_{\overline{b}\in\mathcal{LS}_f} \mathcal{W}_{D_{\overline{b}}f}(\overline{0}) = \sum_{\overline{b}\in\mathcal{LS}_f}\left[\sum_{\overline{x}\in\mathbb{F}_2^n}(-1)^{D_{\overline{b}}f(\overline{x})}\right]\\ &= 2^n \sum_{\overline{b}\in\mathcal{LS}_f}(-1)^{D_{\overline{b}}f(\overline{0})}\end{aligned}$$

□

Lemma 3 stated that if f is a balanced n-variable Boolean function with $\deg(f) = 2$, then there exist a nonzero $\overline{\alpha} \in \mathbb{F}_2^n$ such that $D_{\overline{\alpha}}f(\overline{x}) = f(\overline{x}) \oplus f(\overline{x} \oplus \overline{\alpha}) = 1$ for all $\overline{x} \in \mathbb{F}_2^n$. The proof is given below.

Proof. Let f be a balanced n-variable Boolean function with $\deg(f) = 2$. Since f is balanced, then $\mathcal{W}_f(\overline{0}) = 0$ and consequently $\mathcal{W}_f^2(\overline{0}) = 0$. The result from Proposition 13 implies that the sum $\sum_{\overline{b}\in\mathcal{LS}_f}(-1)^{D_{\overline{b}}f(\overline{0})}$ must be equal to zero. We know that the zero vector $\overline{0} \in \mathbb{F}_2^n$ is a trivial linear structure because $D_{\overline{0}}f(\overline{x}) = 0$ for all $\overline{x} \in \mathbb{F}_2^n$. Clearly $\overline{0} \in \mathcal{LS}_f$. Using existence of zero vector in the set of linear structure of f, then there must exist a vector $\overline{\alpha} \in \mathbb{F}_2^n$, $\overline{\alpha} \neq \overline{0}$ such that $D_{\overline{\alpha}}f(\overline{x}) = 1$ for all $\overline{x} \in \mathbb{F}_2^n$. □

7.2 Linear Structures and Output Differences of an S-Box

Theorem 7. *Let S be an $n \times m$ S-Box and $\Omega_{\overline{\alpha}} = \{\overline{\beta} = (\beta_{m-1}, \ldots, \beta_0) \in \mathbb{F}_2^m \mid$ $\mathbf{Pr}_S[\overline{\alpha} \to \overline{\beta}] > 0\}$ be the set of all possible output differences of S corresponding to input difference $\overline{\alpha} \in \mathbb{F}_2^n$. The vector $\overline{\alpha}$ is a linear structure of the component function $\overline{b} \cdot S(\overline{x})$ if and only if $\overline{b} \cdot \overline{\beta}$ remains equal for all $\overline{\beta} \in \Omega_{\overline{\alpha}}$.*

Proof. Let $h_{m-1}, \ldots, h_0$ be coordinate functions of the S-Box S. For the vector $\overline{b} = (b_{m-1}, \ldots, b_0) \in \mathbb{F}_2^m$ we can express the component function $\overline{b} \cdot S(\overline{x})$ as a linear combination of coordinate functions of S, i.e. $\overline{b} \cdot S(\overline{x}) = b_{m-1}h_{m-1}(\overline{x}) \oplus \ldots \oplus b_0 h_0(\overline{x})$. Since $\overline{\alpha} \in \mathbb{F}_2^n$ is a linear structure of $\overline{b} \cdot S(\overline{x})$, we have the following

$$\begin{aligned}
&c = \overline{b} \cdot S(\overline{x}) \oplus \overline{b} \cdot S(\overline{x} \oplus \overline{\alpha}) && \forall \overline{x} \in \mathbb{F}_2^n \\
&c = (b_{m-1}h_{m-1}(\overline{x}) \oplus \ldots \oplus b_0 h_0(\overline{x})) \oplus \\
&\qquad (b_{m-1}h_{m-1}(\overline{x} \oplus \overline{\alpha}) \oplus \ldots \oplus b_0 h_0(\overline{x} \oplus \overline{\alpha})) && \forall \overline{x} \in \mathbb{F}_2^n \\
&c = b_{m-1}(h_{m-1}(\overline{x}) \oplus h_{m-1}(\overline{x} \oplus \overline{\alpha})) \oplus \ldots \oplus b_0(h_0(\overline{x}) \oplus h_0(\overline{x} \oplus \overline{\alpha})) && \forall \overline{x} \in \mathbb{F}_2^n \\
&c = \overline{b} \cdot (h_{m-1}(\overline{x}) \oplus h_{m-1}(\overline{x} \oplus \overline{\alpha}), \ldots, h_0(\overline{x}) \oplus h_0(\overline{x} \oplus \overline{\alpha})) && \forall \overline{x} \in \mathbb{F}_2^n \\
&c = \overline{b} \cdot \overline{\beta} && \forall \overline{\beta} \in \Omega_{\overline{\alpha}}
\end{aligned}$$

The converse is obvious from above equations. □

7.3 DDT of the S-Box of PRESENT

Table 3. Difference Distribution Table of the S-Box of PRESENT

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	4	0	0	0	4	0	4	0	0	0	4	0	0
2	0	0	0	2	0	4	2	0	0	0	2	0	2	2	2	0
3	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
4	0	0	0	0	0	4	2	2	0	2	2	0	2	0	2	0
5	0	2	0	0	2	0	0	0	0	2	2	2	4	2	0	0
6	0	0	2	0	0	0	2	0	2	0	0	4	2	0	0	4
7	0	4	2	0	0	0	2	0	2	0	0	0	2	0	0	4
8	0	0	0	2	0	0	0	2	0	2	0	4	0	2	0	4
9	0	0	2	0	4	0	2	0	2	0	0	0	2	0	4	0
10	0	0	2	2	0	4	0	0	2	0	2	0	0	2	2	0
11	0	2	0	0	2	0	0	0	4	2	2	2	0	2	0	0
12	0	0	2	0	0	4	0	2	2	2	2	0	0	0	2	0
13	0	2	4	2	2	0	0	2	0	0	2	2	0	0	0	0
14	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
15	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4