Redefining the Transparency Order

Kaushik Chakraborty, Subhamoy Maitra, Sumanta Sarkar, Bodhisatwa Mazumdar, Debdeep Mukhopadhyay

Indian Statistical Institute, Kolkata and Indian Institute of Technology, Kharagpur
Emails: kaushik.chakraborty9@gmail.com, subho@isical.ac.in, sumanta.sarkar@gmail.com, bm.iitkgp@gmail.com, debdeep.mukhopadhyay@gmail.com

Abstract. In this paper, we consider the multi-bit Differential Power Analysis (DPA) in the Hamming weight model. In this regard, we revisit the definition of Transparency Order (TO) from the work of Prouff (FSE 2005) and find that the definition has certain limitations. Although this work has been quite well referred in the literature, surprisingly, these limitations remained unexplored for almost a decade. The existing definition of TO (by Prouff) for an S-box $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ considers maximization on $\beta \in \mathbb{F}_2^m$. However, we show that the expression suggested by Prouff is always maximum when β is either all-zero or all-one, that makes the maximization over all $\beta \in \mathbb{F}_2^m$ redundant. Digging TO deeper, we note that the existing definition of TO assumes certain cross-correlation terms between the co-ordinate Boolean functions of F as zero. This is not true in general and thus we need to accommodate these terms in the definition. Further the definition is based on the assumption that the co-ordinate functions in the S-boxes are balanced (which is indeed logical for practical S-boxes), but unfortunately the measure has been calculated for bent functions (which are not balanced) in Prouff's paper and subsequent works. We analyse the definition from scratch, modify it and finally provide a substantially improved and logical definition that can theoretically capture DPA in Hamming weight model for hardware implementation with precharge logic. In this regard, our analysis comes with numerical data for AES S-Box and the family of S-Boxes described in the context of Prince.

Keywords: AES, Auto-correlation, Cross-correlation, Differential Power Analysis, Prince, S-Box, Transparency Order, Walsh Spectrum.

1 Introduction

Differential Power Analysis (DPA) is one of the strongest forms of side-channel attacks in which the information about the secret key is leaked through power traces while the encryption is executing on the cryptographic platform. The efficiency of these attacks is naturally much higher than linear or differential cryptanalysis due to the information related to the power traces. To resist such attacks, though algorithmic countermeasures [16] like masking and leakage resistant logic exist, that may lead to increased footprint on the implementation platforms in terms of area and power consumptions. It should also be noted that sometimes masked implementations can also be attacked [10]. With this backdrop, it is evident that the S-boxes in block ciphers would be the prime target of DPA. From the designers point of view, the S-boxes should be chosen carefully such that they should have high DPA resilience in addition to the resistance to other classical cryptanalytic attacks like linear and differential cryptanalysis.

In [7], the theoretical resistance of AES and DES S-boxes to linear cryptanalysis vis a vis DPA attacks in terms of signal-to-noise ratio (SNR) was investigated. Then, an attempt to quantify the DPA resilience of the S-boxes was made in [13], where the parameter Transparency Order (TO) was introduced. This was an important attempt in defining a metric for the DPA resilience of

S-boxes for almost a decade ago. The paper [13] tried to explain that S-boxes with smaller TO have higher DPA resilience. The TO, as defined in [13] was found to depend on the propagation characteristics (PC) of the co-ordinate functions of the S-boxes. The bent functions that satisfy the PC for all orders have been found to have worst TO value (though we show in this paper that by the definition of [13], TO cannot be measured for a bent function), while the linear S-boxes have the best DPA resilience. However, the linear S-boxes are not acceptable as a secure cryptographic primitive. Further analysis of TO, as defined in [13], has been followed in [5, 11]. The main issue here lies in the fact that a redundant definition of transparency order has received significant attention in literature and for almost a decade the problem in the definition remained unidentified. This paper points out to the problems in the definition of transparency order and provides further measures for better modelling of DPA.

Differential Power Analysis (DPA) is one kind of side channel attack that exploits the difference between the power consumed by a single gate when its output changes from zero to one or vice versa. Initial results in this direction have been presented by Kocher et al [9]. Suppose the attacker has a sufficiently large collection of ciphertexts $E_{\dot{K}}(x)$, where $\dot{K}$ is the round key, E denotes the encryption function and x denotes the corresponding plaintext. First, the sample power consumption traces $T_x(t)$ (it could be a series of power related data based on time or may be a summarized data related to power) are collected for a sufficient number of plaintexts x. These samples actually give the information about the power consumed by each gate when output changes. One may note that to collect the sample of power consumption traces, the attacker doesn't need any information about the plaintexts. It is enough if the attacker records the power consumption during the computation of encryption function E. Next, based on these power traces, the actual attack can be mounted off-line.

In single bit DPA attack, a particular bit j is considered and the attacker tries to make a distinguisher by partitioning the power traces in two bins by considering whether the bit value is zero or one, corresponding to the key guessed. Let $\dot{K}$ be the actual round key used for encryption. The attacker guesses a round key K and then the traces are assigned in either of the two bins, say S_0 and S_1, according to the bit value of j. One can compute the Differential Trace [7], denoted by $D_{T,K,j}$ as $D_{T,K,j}(t) = \frac{1}{|S_1|}\sum_{T_x \in S_1} T_x(t) - \frac{1}{|S_0|}\sum_{T_x \in S_0} T_x(t)$. The quantity $D_{T,K,j}(t)$ works as a distinguisher in the single bit power attack model. According to the theory proposed in [9] the distribution $D_{T,K,j}(t)$ should show a peak for the correct key $K = \dot{K}$.

In single bit DPA attack, the sets S_0 and S_1 are constructed on the basis of a fixed bit j. One can also measure the distribution $D_{T,K,j}$ considering different j's. This kind of DPA attack is called multi-bit DPA attack. It works as follows. For each of the guessed key K the quantity $D_{T,K,j}$ is computed for all $1 \leq j \leq m$. Then one can compute the quantity, $D_{T,K}$, which considers proper accumulation of $D_{T,K,j}(t)$ values for all j. Here $D_{T,K}$ works as a distinguisher and similar to the single bit case, the graphical presentation of $D_{T,K}$ provides a peak if $K = \dot{K}$, which should not be observed for a wrong guess. This is the base model for the work presented in this paper. Before proceeding further, let us introduce a few basic concepts related to Boolean functions.

1.1 Basics of Boolean functions

Let $\mathbb{F}_2^n$ be the vector space that contains all the n-bit binary vectors. A (single output) Boolean function on n variables may be viewed as a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. We will denote the set of n-variable Boolean functions as $\mathcal{B}_n$. It is easy to note that $|\mathcal{B}_n| = 2^{2^n}$.

The support of a Boolean function f is defined as $Supp(f) = \{x \in \mathbb{F}_2^n | f(x) = 1\}$. When we use a Boolean function as a cryptographic primitive, we generally consider the functions which output 0 and 1 with equal probability. Thus, we generally consider functions in $\mathcal{B}_n$ for which the cardinality of the support is 2^{n-1}. These are known as balanced functions.

Let $x = (x_1, \ldots, x_n)$ and $\omega = (\omega_1, \ldots, \omega_n)$ both belong to $\mathbb{F}_2^n$ and the inner product $x \cdot \omega = x_1\omega_1 \oplus \cdots \oplus x_n\omega_n$. The Walsh transform of $f(x)$ is an integer valued function over $\mathbb{F}_2^n$ which is defined as $W_f(\omega) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus x \cdot \omega}$. The autocorrelation transform of $f(x)$ is again an integer valued function over $\mathbb{F}_2^n$ which is defined as $\mathcal{A}_f(\omega) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus f(x \oplus \omega)}$. The Walsh and autocorrelation spectra are important properties in designing Boolean functions that may be used as cryptographic primitives. In general, it is expected that the maximum absolute value in any of these spectra should be low for better resistance against cryptanalysis.

An S-box can be seen as a multi-output Boolean function. As we have discussed, an $n \times m$ S-box is a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Let $u \cdot F$, where $u \in \mathbb{F}_2^m$. By $H(u)$, we mean the number of 1's in the binary representation of u.

Let $u = (u_1, \ldots, u_m)$, with $H(u) = 1$, where $u_1 = \ldots = u_{j-1} = u_{j+1} = \ldots = u_m = 0$ and $u_j = 1$. Each component function of the S-box is a single output Boolean function $u \cdot F$, where $u \in \mathbb{F}_2^m$ and $H(u) = 1$. If $F = (F_1, \ldots, F_m)$, then one may note that $u \cdot F = F_j$. By abuse of notation, we may also denote this component function as F_u. That is, the notations F_u and F_j are used interchangeably for a component function in this draft.

Given $f_1, f_2 \in \mathcal{B}_n$, we define the cross-correlation spectrum between these functions as $\mathcal{C}_{f_1,f_2}(\omega) = \sum_{x \in \{0,1\}^n} (-1)^{f_1(x) \oplus f_2(x \oplus \omega)}$. In fact, in [13], the cross-correlation terms have been ignored while calculating the TO. We show that these terms are significant and cannot be ignored.

1.2 DPA Attack and Transparency Order of S-Boxes

As discussed, the DPA provides the attacker a verifier or distinguisher to guess the correct key. The distinguisher based on the differential traces works on the hypothesis that for the correct key it takes the maximum value (though, due to the presence of system noises one can get several other "ghost peaks" for wrong keys). Now, from the designer's point of view, one should design the S-boxes in such a manner so that the distribution of the differential trace becomes almost uniform. In such a case, the correct key cannot be distinguished from a wrong key. This gives a security criterion for designing the S-boxes.

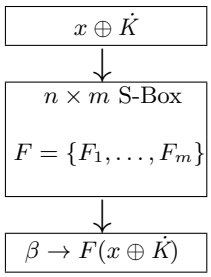

Fig. 1. Model of DPA on an S-Box. In the output the previous value is β, which is updated by $F(x \oplus \dot{K})$.

In [7], a few ideas were presented to measure the efficiency of DPA on an S-box. They studied single bit DPA in the Hamming distance model, introduced in [4]. Let F be an $n \times m$ S-box. Given

$v, \beta \in \mathbb{F}_2^m$, and $H(v) = 1$, we can consider $\Delta_{K,\dot{K}}$ for single bit DPA as

$$\Delta_{K,\dot{K}}(v,\beta) = \frac{1}{2^n} \sum_{\substack{u \in \mathbb{F}_2^m \\ H(u)=1}} \sum_{x \in \{0,1\}^n} (-1)^{F_v(x \oplus K) \oplus \left(F_u(x \oplus \dot{K}) \oplus \beta \cdot u\right)}.$$

If $v_j = 1$ (the rest of the bits are zero as $H(v) = 1$), then the quantity $D_{T,K,j}$ is being calculated here. The quantity β comes with the system. It denotes the temporary value of the register, which is replaced by $E_K(x) = F(x \oplus K)$.

Informally speaking, the TO is used to quantify the resistance of S-boxes towards DPA attacks which employ Difference of Means (DoM) model. To resist DPA attacks, the bias value of DoMs should be small for any round key $\dot{K}$. The parameter is defined in terms of initial state value which is constant (say $\beta \in \{0,1\}^m$) for platforms like embedded smart cards based on precharge logic. The precharge logic is used in case of microcontrollers in which there is a precharge phase where in the initial part of the clock cycle the registers are initialized to some fixed value in each round. That is, given the precharge logic assumption for the hardware design, β is considered to be a constant.

According to this definition as given in [13], if some S-box shows low TO, then that S-box is more resistant against DPA attack, i.e., the number of power traces to identify the correct key will be higher. One can easily check that the TO becomes minimum for the S-boxes for which the co-ordinate Boolean functions become constant or affine and on the other hand, the highly nonlinear S-boxes have higher transparency order, implying that they are more susceptible to DPA attacks. Though the linear S-boxes are good in terms of TO, linear S-boxes cannot be used for cryptographic reasons and thus we have to mainly study the behaviour of TO for the well known nonlinear S-boxes used in practice. The TO values of constant or linear S-boxes are actually of little interest, though those values may be computed for noting the bounds on TO.

In [13], Prouff formalized the definition of transparency order in multi-bit scenario. After certain assumptions, for an $n \times m$ S-box $F = (F_1, \ldots, F_m)$, the final formula for the transparency order (TO) as in [13] is given by

$$\tau_F = \max_{\beta \in \mathbb{F}_2^n} \left(|m - 2H(\beta)| - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} |\sum_{i=1}^{m} (-1)^{\beta_i} \mathcal{A}_{F_i}(a)| \right). \tag{1}$$

We critically study the above definition in this paper. The organization of our paper is as follows. In the next section (Section 2), we show that this definition has redundancy in terms of considering the maximum over all $\beta \in \mathbb{F}_2^m$. Then in Section 3 we critically analyse the definition of TO in Hamming weight model from the basic background and identify all the limitations of the existing definition [13]. Next, in Section 4, we present our modified definition of TO that explains the DPA in Hamming weight model more appropriately than [13] (see also Remark 1). Section 5 concludes the paper. We also provide Appendices A, B and C for some detailed calculations, bounds and examples.

Having a good TO is indeed not a determinant criterion for a cryptographically secure S-Box. Nevertheless, it provides clear comparison between two S-boxes having the same cryptographic parameters (e.g., one may consider our analysis in this paper that clearly shows the difference in quality of several 4×4 S-boxes studied in the context of Prince [3]). Thus, a correct definition of TO is of importance to choose between good S-boxes and then deciding whether the chosen one

can be protected against Side Channel Attacks (SCA) at a reasonable cost (for example, by higher order masking as studied in [15]). In this direction, threshold implementation related results for all the 3×3 and 4×4 S-boxes have been presented in [2].

Other than DPA with Hamming weight model in precharge logic scenario, that we concentrate on in this paper, there are several models for SCA. Other possible leakages such as glitches have been studied in [10, 12]. Recently, the notion of confusion coefficient has been presented in [6]. Further the notion of transparency metric has been studied in [8]. A metric to consider the side channel distinguisher, known as relative distinguishing margin has been presented and studied in [17, 18] and certain clarifications on this has been made in [14]. We refer these papers and the references therein for recent state of the art developments in DPA under several models.

2 Redundant Definition of Transparency Order [13]

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. We explain the definition of the transparency order [13] τ_F of $F = (F_1, \ldots, F_m)$ in a step by step manner for a better understanding. Let $\alpha \in \mathbb{F}_2^n$ and $\beta \in \mathbb{F}_2^m$. Let us denote

$$\nu_{F,\beta} = \frac{1}{2^{2n} - 2^n} \sum_{\alpha \in \mathbb{F}_2^{n^*}} |\sum_{i=1}^{m} (-1)^{\beta_i} \mathcal{A}_{F_i}(\alpha)|. \tag{2}$$

and

$$\mu_{F,\beta} = |m - 2H(\beta)| - \nu_{F,\beta}. \tag{3}$$

The TO of the function F is

$$\tau_F = \max_{\beta \in \mathbb{F}_2^m} \mu_{F,\beta}. \tag{4}$$

Proposition 1. $\mu_{F,\beta} = \mu_{F,\overline{\beta}}$.

Proof. Note that $|m - 2H(\beta)| = |m - 2(m - H(\overline{\beta}))| = |-m + 2H(\overline{\beta})| = |m - 2H(\overline{\beta})|$.

One may also check that $\nu_{F,\beta} = \nu_{F,\overline{\beta}}$. This is as follows.

$$\begin{aligned}\nu_{F,\beta} &= \frac{1}{2^{2n} - 2^n} \sum_{\alpha \in \mathbb{F}_2^{n^*}} |\sum_{i=1}^{m} (-1)^{\beta_i} \mathcal{A}_{F_i}(\alpha)| = \frac{1}{2^{2n} - 2^n} \sum_{\alpha \in \mathbb{F}_2^{n^*}} |\sum_{i=1}^{m} - \Big((-1)^{\beta_i} \mathcal{A}_{F_i}(\alpha)\Big)| \\ &= \frac{1}{2^{2n} - 2^n} \sum_{\alpha \in \mathbb{F}_2^{n^*}} |\sum_{i=1}^{m} \Big((-1)^{\overline{\beta}_i} \mathcal{A}_{F_i}(\alpha)\Big)| = \nu_{F,\overline{\beta}}\end{aligned}$$

Thus the proof. □

Next we present the most important result in this direction.

Proposition 2. *Let* $0 < H(\beta) \leq \lfloor \frac{m}{2} \rfloor$. *Then* $\mu_{F,\beta} \leq \mu_{F,\mathbf{0}}$.

Proof. Consider that $0 < k = H(\beta) \leq \lfloor \frac{m}{2} \rfloor$. Now, $\mu_{F,\mathbf{0}} = (m - \nu_{F,\mathbf{0}})$ and $\mu_{F,\beta} = (m - 2k - \nu_{F,\beta})$.

Let, in contrary to the statement of the proposition, $\mu_{F,\beta} > \mu_{F,\mathbf{0}}$. Then $\nu_{F,\mathbf{0}} - \nu_{F,\beta} > 2k$, i.e.,

$$\sum_{\alpha \in \mathbb{F}_2^{n^*}} \left[|\sum_{i=1}^{m} (\mathcal{A}_{F_i}(\alpha))| - |\sum_{i=1}^{m} \Big((-1)^{\beta_i} \mathcal{A}_{F_i}(\alpha)\Big)| \right] > (2^{2n} - 2^n) 2k.$$

Let $S = \{1, 2, \ldots, m\}$ and $T \subseteq S$, such that $i \in T$ if and only if $\beta_i = 1$. That is T is the support of β.

Then we can rewrite the above inequality as

$$\sum_{\alpha \in \mathbb{F}_2^{n^*}} \left[|\sum_{i=1}^{m} (\mathcal{A}_{F_i}(\alpha))| - |\sum_{i \in S \setminus T} (\mathcal{A}_{F_i}(\alpha)) - \sum_{i \in T} (\mathcal{A}_{F_i}(\alpha))| \right] > (2^{2n} - 2^n)2k.$$

Using the inequality $|x| - |y| \leq |x - y|$, we obtain,

$$\sum_{\alpha \in \mathbb{F}_2^{n^*}} \left[|\sum_{i=1}^{m} (\mathcal{A}_{F_i}(\alpha)) - \sum_{i \in S \setminus T} (\mathcal{A}_{F_i}(\alpha)) + \sum_{i \in T} (\mathcal{A}_{F_i}(\alpha))| \right] > (2^{2n} - 2^n)2k,$$

$$\text{i.e., } \sum_{\alpha \in \mathbb{F}_2^{n^*}} 2 \left| \sum_{i \in T} (\mathcal{A}_{F_i}(\alpha)) \right| > (2^{2n} - 2^n)2k.$$

We know that $|\mathcal{A}_{F_i}(\alpha)| \leq 2^n$, and thus we land into a contradiction as the left hand side is always less than or equal to the right hand side. (Even taking the maximum value 2^n, we get that the left hand side is equal, but cannot be greater than the right hand side.) Thus the proof. □

Therefore, we have the following result that shows that the definition of transparency order is actually redundant and it does not depend on β. The proof follows from Propositions 1, 2.

Theorem 1. $\tau_F = \mu_{F,\mathbf{0}} = m - \frac{1}{2^{2n} - 2^n} \sum_{\alpha \in \mathbb{F}_2^{n^*}} |\sum_{i=1}^{m} \mathcal{A}_{F_i}(\alpha)|$.

3 Critically analysing the TO for Multi-bit DPA Attack

Given the redundancy in the definition of TO as in [13], we look into the definition from the basic principle and obtain various other limitations of the definition. We highlight several assumptions considered in [13] and critically comment on those.

Referring to Figure 1, the output of the S-box becomes $F(x \oplus \dot{K})$ from β, where β is the precharge logic value that is fixed with the system, i.e., β is constant. So, the number of bits, changed after storing the S-box output bits is $H(F(x \oplus \dot{K}) \oplus \beta)$ The basic idea of DPA works as follows.

Given the correct key $\dot{K}$ (the attacker does not know this), the power trace of the encryption or decryption can be collected by the adversary corresponding to the known plaintexts. As the corresponding $n \times m$ S-boxes are in general not very large, one may expect that the power traces are available corresponding to all the 2^n possible inputs x. After the data is available, the attack may work off-line where the attacker tries each of the possible 2^n keys K (these are actually parts of round keys that are XORed with x) and partitions the power traces in two bins. It is expected that for the correct key $\dot{K}$, the partitioning will show some distinguishing feature than that in the case of the incorrect keys.

Let us concentrate on the j-th output bit of the S-box. Given any key K (which may or may not be $\dot{K}$), we put the power related information in two bins depending on the value of $F_j(x \oplus K)$. As in [13], for theoretical analysis, the Hamming weight of $F(x \oplus K) \oplus \beta$ can be considered as a logical model for the power related information. The difference of average value in the two bins is

$$\Delta_{K,\dot{K}}(j, \beta) = \frac{1}{|S_{K,1}|} \sum_{x \in S_{K,1}} H\left(F(x \oplus \dot{K}) \oplus \beta\right) - \frac{1}{|S_{K,0}|} \sum_{x \in S_{K,0}} H\left(F(x \oplus \dot{K}) \oplus \beta\right), \quad (5)$$

where $S_{K,0} = \{x|F_j(x \oplus K) = 0\}$ and $S_{K,1} = \{x|F_j(x \oplus K) = 1\}$. At this point let us present a technical result.

Proposition 3. *Let us fix $\beta \in \mathbb{F}_2^m$. Let $F = (F_1, \ldots, F_m)$ be an $n \times m$ S-box (i.e., $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$). Let the co-ordinate functions be such that they are pairwise complement when m is even. In case m is odd, then we consider $\frac{m-1}{2}$ pairs of pairwise complement functions and one constant function. For any such S-box, $\Delta_{K,\dot{K}}(j, \beta) = 0$ for any j, $1 \leq j \leq m$.*

Proof. The proof follows by noting that $H(F(x))$ is constant for all $x \in \mathbb{F}_2^n$. Thus it is immediate to note that $H\left(F(x \oplus \dot{K}) \oplus \beta\right)$ is always constant making $\Delta_{K,\dot{K}}(j, \beta) = 0$, for any j and the fixed β. □

Consider a special case when m is even. For any such S-box, where all the functions are taken to be pairwise complement and bent, no DPA is possible under the model we are working on. However, the measure presented in [13, 5] shows that the TO is the maximum (i.e., m) for such functions, which means that they are maximally prone to such DPA. The conclusion in [13, 5] is not correct and it happened due to certain assumptions that make the definition of TO invalid for S-boxes with unbalanced co-ordinate functions such as bent.

Assumption 1. The analysis of [13] implicitly assumes that the co-ordinate functions of the S-box are balanced.

Note that, if F_j is not balanced, then handling the terms in (5) becomes complicated. Interestingly, the definition used in [13, Definition 2] considered the balancedness implicitly. However, they had later measured the transparency order of bent functions in [13, Theorem 1], and did not note that the bent functions are indeed not balanced. Similarly, transparency order of bent functions have been incorrectly studied later in [5]. To clarify the situation, below we show how the assumption that the coordinate functions are balanced lead to the definition of transparency order.

If F_j is balanced, then $|S_{K,0}| = |S_{K,1}| = 2^{n-1}$ and one can show (see (24) in Appendix A for details)

$$\Delta_{K,\dot{K}}(j, \beta) = -\frac{m}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{F_j(x \oplus K)} + \frac{1}{2^n} \sum_{i=1}^{m} (-1)^{\beta_i} \sum_{x \in \mathbb{F}_2^n} (-1)^{F_j(x \oplus K) \oplus F_i(x \oplus \dot{K})}.$$

As the first term of right hand side will vanish due to Assumption 1 on balancedness of the co-ordinate functions, we obtain

$$\Delta_{K,\dot{K}}(j, \beta) = \frac{1}{2^n} \sum_{i=1}^{m} (-1)^{\beta_i} \sum_{x \in \mathbb{F}_2^n} (-1)^{F_j(x \oplus K) \oplus F_i(x \oplus \dot{K})}. \tag{6}$$

As explained above (and also in [13]), the correlation between $F(x \oplus \dot{K}) \oplus \beta$ and $F(x \oplus K)$ is measured for each key given all possible input x to the S-box. We need to derive the values of $\Delta_{K,\dot{K}}(j, \beta)$ for two cases, namely, $K = \dot{K}$ and $K \neq \dot{K}$.

Assumption 2. The analysis of [13] assumes that $F_i \oplus F_j$ is balanced for all i and the fixed j.

In general, we obtain (see (25) in Appendix A for details)

$$\Delta_{K,\dot{K}}(j,\beta) = \frac{1}{2^n}\left((-1)^{\beta_j}\mathcal{A}_{F_j}(K\oplus\dot{K}) + \sum_{i=1,i\neq j}^{m}(-1)^{\beta_i}\mathcal{C}_{F_i,F_j}(K\oplus\dot{K})\right). \tag{7}$$

Thus, for $K = \dot{K}$, we have

$$\Delta_{\dot{K},\dot{K}}(j,\beta) = (-1)^{\beta_j} + \frac{1}{2^n}\sum_{i=1,i\neq j}^{m}(-1)^{\beta_i}\mathcal{C}_{F_i,F_j}(0). \tag{8}$$

Note that, if $F_i \oplus F_j$ is balanced for all i and the fixed j, then $\mathcal{C}_{F_i,F_j}(0) = 0$ and thus, $\Delta_{\dot{K},\dot{K}}(j,\beta) = (-1)^{\beta_j}$. In fact, if one considers an $n \times n$ S-box which is a permutation (e.g., the 8×8 S-box used in AES), then $\mathcal{C}_{F_i,F_j}(0)$ is always zero.

One may note that Assumptions 1 and 2 are satisfied when the involved (n, m) S-box is balanced (which is the case of the vast majority of cryptographic S-boxes).

In single bit DPA attack the expression $\Delta_{K,\dot{K}}(j,\beta)$ is calculated for all possible pairs $(K, \dot{K})$ for a fixed j. Here j denotes the position of the co-ordinate function of the S-box, where the power trace is observed. In case of multi-bit differential power attack this j varies for all co-ordinate functions, i.e., j varies from 1 to m. Thus, the following quantity $\delta_{K,\dot{K}}$ has been defined for multi-bit DPA as follows [13, Equation (10)]:

$$\delta_{K,\dot{K}}(\beta) = |\sum_{j=1}^{m}\Delta_{K,\dot{K}}(j,\beta)|. \tag{9}$$

We would like to point out that this definition has the problem in properly modelling multi-bit DPA attack as well as in the final expression of TO, for taking the absolute value after making the sum. This will always make the TO maximum at all-zero or all-one point. We will later revisit this definition by considering the quantity $\sum_{j=1}^{m}|\Delta_{K,\dot{K}}(j,\beta)|$.

For the case $K = \dot{K}$ we have,

$$\delta_{\dot{K},\dot{K}}(\beta) = \left|\sum_{j=1}^{m}\left((-1)^{\beta_j} + \frac{1}{2^n}\sum_{i=1,i\neq j}^{m}(-1)^{\beta_i}\mathcal{C}_{F_i,F_j}(0)\right)\right|.$$

Given Assumption 2, we have

$$\delta_{\dot{K},\dot{K}}(\beta) = \left|\sum_{j=1}^{m}(-1)^{\beta_j}\right| = |m - 2H(\beta)|. \tag{10}$$

For $K \neq \dot{K}$, we have,

$$\delta_{K,\dot{K}}(\beta) = \frac{1}{2^n}\left|\sum_{j=1}^{m}\left((-1)^{\beta_j}\mathcal{A}_{F_j}(K\oplus\dot{K}) + \sum_{i=1,i\neq j}^{m}(-1)^{\beta_i}\mathcal{C}_{F_i,F_j}(K\oplus\dot{K})\right)\right|. \tag{11}$$

Assumption 3. The analysis of [13] assumes that $\mathcal{C}_{F_i,F_j}(K\oplus\dot{K})$ can be considered to be zero for all the cases making certain assumptions on independence.

Note that, this is not true as we cannot have all the values zero in cross-correlation spectrum in general. In fact, we will later present a detailed study for the 8×8 S-box used in AES that will clearly show the limitation of the Assumption 3 made in [13].

Given Assumption 3, we have

$$\delta_{K,\dot{K}}(\beta) = \frac{1}{2^n} \left| \sum_{j=1}^{m} (-1)^{\beta_j} \mathcal{A}_{F_j}(K \oplus \dot{K}) \right|. \tag{12}$$

In the case of the multi-bit DPA attack, for all possible pairs of keys $(K, \dot{K})$, one can compute the values of $\delta_{K,\dot{K}}(\beta)$. It is expected that if $K = \dot{K}$, then $\delta_{K,\dot{K}}$ takes the maximum value for some β. From the designer's point of view, the S-boxes should be chosen in such a manner so that for other pairs $(K, \dot{K})$, the values of $\delta_{K,\dot{K}}(\beta)$ do not deviate much from the value of $\delta_{\dot{K},\dot{K}}(\beta)$ for resistance against DPA. Thus, the TO is defined as follows in [13]:

$$\tau_F = \max_{\beta \in \mathbb{F}_2^n} \tau_F^{\beta}, \text{ where, } \tau_F^{\beta} = \left(\frac{1}{2^n - 1} \sum_{\substack{K \in F_2^n \\ K \neq \dot{K}}} \Big(\delta_{\dot{K},\dot{K}}(\beta) - \delta_{K,\dot{K}}(\beta) \Big) \right). \tag{13}$$

Suppose $K \oplus \dot{K} = a$. Then by substituting the values of $\delta_{\dot{K},\dot{K}}$ from (10) and $\delta_{K,\dot{K}}$ from (12), we get

$$\tau_F^{\beta} = |m - 2H(\beta)| - \frac{1}{2^n(2^n - 1)} \sum_{a \in \mathbb{F}_2^{n*}} \left| \sum_{j=1}^{m} (-1)^{\beta_j} \mathcal{A}_{F_j}(a) \right|, \tag{14}$$

and thus,

$$\tau_F = \max_{\beta \in \mathbb{F}_2^m} \left(|m - 2H(\beta)| - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \left| \sum_{j=1}^{m} (-1)^{\beta_j} \mathcal{A}_{F_j}(a) \right| \right), \tag{15}$$

which is the same as (1) presented in [13]. As we have described, the work in [13] considered a few assumptions, but several critical comments can be made on that. To be specific, we point out the following.

- Assumption 1 is logical and it works for practical S-boxes that the co-ordinate Boolean functions are balanced. However, given this assumption, it is not possible to consider unbalanced co-ordinate functions in the S-box under this definition. However, this had been improperly done in [13, 5] in concluding certain results related to bent functions.
- Assumption 2 is also logical in the sense that it is quite practical to consider that the XOR of two co-ordinate functions should be balanced.
- Assumption 3 considers that the cross-correlation spectrum between two co-ordinate functions will contain all zero values due to certain independence. This is indeed not correct and one should specifically calculate these value that we will also present here. As example, for the 8×8 S-box used in AES, the values in the spectrum are indeed significant. Ignoring this significance led to the redundant definition of τ_F in [13] where it does not depend on β at all as we have described in Section 2.

3.1 Considering the cross-correlation terms

For a proper measure, we need to add the cross-correlation terms as given in (11). Thus, we should consider the following definition for further investigation in this area.

$$\tau'^{\beta}_{F} = |m - 2H(\beta)| - \frac{1}{2^n(2^n-1)} \sum_{a \in \mathbb{F}_2^{n^*}} \left| \sum_{j=1}^{m} \left((-1)^{\beta_j} \mathcal{A}_{F_j}(a) + \sum_{i=1, i \neq j}^{m} (-1)^{\beta_i} \mathcal{C}_{F_i,F_j}(a) \right) \right|. \tag{16}$$

Similar to Proposition 1, one may note that under the modified definition of τ'^{β}_{F} as given in (16), τ'^{β}_{F} and $\tau'^{\overline{\beta}}_{F}$ are equal (see (26) in Appendix A for details). Let us now consider τ'_F as in (17). This definition will only be valid for the $n \times m$ S-boxes $F = (F_1, \ldots, F_m)$, where each co-ordinate function F_i and further the functions $F_i \oplus F_j$ for $0 \leq i \neq j \leq m$ are balanced.

$$\tau'_F = \max_{\beta \in \mathbb{F}_2^m} \left(|m - 2H(\beta)| - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n^*}} \left| \sum_{j=1}^{m} \left((-1)^{\beta_j} \mathcal{A}_{F_j}(a) + \sum_{i=1, i \neq j}^{m} (-1)^{\beta_i} \mathcal{C}_{F_i,F_j}(a) \right) \right| \right) \tag{17}$$

Unfortunately, similar to (15), this definition also becomes redundant for cryptographically strong S-boxes. This is because, the magnitude of the values in autocorrelation and cross-correlation spectra of cryptographically strong n-variable Boolean functions are of the order of $2^{\frac{n}{2}}$. Thus, the term $|m - 2H(\beta)|$ will dominate hugely and naturally it will be maximum when β has all-zero or all-one pattern.

Now consider the definition from cryptanalysts' viewpoint. The power traces will be available to the attacker and she can analyse the data off-line to guess the correct key. Thus, the attacker will try to use the power traces in such a way so that the correct key $\dot{K}$ can be distinguished from the other keys.

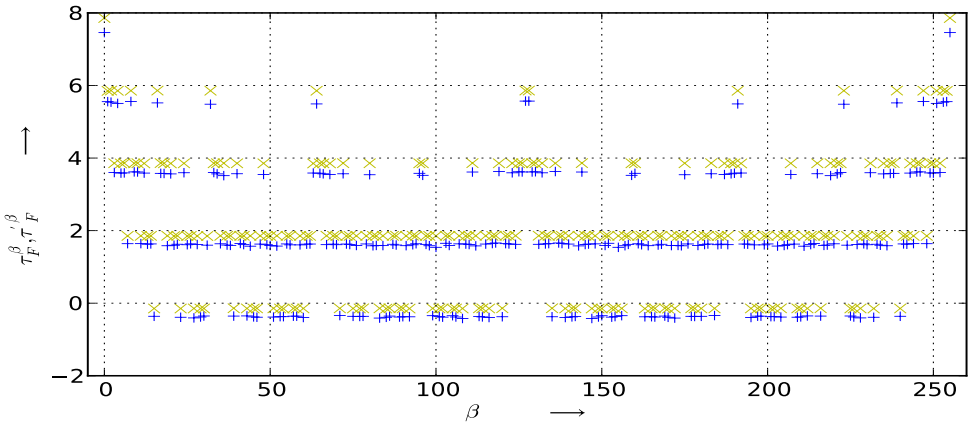

Fig. 2. Values of τ_F^{β} (in Yellow) and τ'^{β}_F (in Blue) as β varies over $\mathbb{F}_2^8$ for AES S-box. The 8-bit patterns of β are written as their integer values.

In Figure 2, for AES S-box, we show the values of τ_F^{β} and ${\tau'}_F^{\beta}$ for different values of β. The figure shows that for some values of β, τ_F^{β} and $\tau_F^{\overline{\beta}}$ are negative. This implies that for those values of β, $\delta_{K,\dot{K}}(\beta)$ is not maximum when $K = \dot{K}$. The negative value of average deviation of $\delta_{K,\dot{K}}(\beta)$ with respect to $\delta_{\dot{K},\dot{K}}(\beta)$ indicates that for some K, $\delta_{\dot{K},\dot{K}}(\beta) < \delta_{K,\dot{K}}(\beta)$. (There are some K for which $\delta_{\dot{K},\dot{K}}(\beta) > \delta_{K,\dot{K}}(\beta)$ too). This phenomenon prevents the attacker to guess the correct key. This happens due to considering the absolute value after taking the sum of $\Delta_{K,\dot{K}}(j,\beta)$ for different j's in [13] (see also (9)). Note that if the precharge logic β is indeed all-zero or all-one, then the existing idea of [13] works well. However, as $H(\beta)$ becomes closer to $\frac{m}{2}$, the term $|m-2H(\beta)|$ reduces substantially, making τ_F^{β} and ${\tau'}_F^{\beta}$ negative in some cases, that makes the definition unacceptable from cryptanalytic point of view.

4 Redefining TO: where to take the absolute values

As explained before (5), we try to identify the correct key from power related information and thus the quantity $\Delta_{K,\dot{K}}(j,\beta)$ has been defined to model that. When we extend that for multiple bits, from cryptanalysts' point of view, we want to add the absolute values to identify the correct key with better confidence for any β. This motivates us to revisit the definition in (9) and we provide the modified definition that models the practical situation more logically.

$$\underline{\delta}_{K,\dot{K}}(\beta) = \sum_{j=1}^{m} |\Delta_{K,\dot{K}}(j,\beta)|. \tag{18}$$

Let us continue our analysis with this definition in (18). With this the value of $\underline{\delta}_{\dot{K},\dot{K}}(\beta)$ as in (10) is updated as:

$$\underline{\delta}_{\dot{K},\dot{K}}(\beta) = \sum_{j=1}^{m} |(-1)^{\beta_j}| = m. \tag{19}$$

Note that the term related to $H(\beta)$ is removed in this case. This is indeed important as otherwise this Hamming weight of β was influencing the complete measure without any real justification and making the definition redundant by maximizing it for all-zero or all-one β.

For the cases $K \neq \dot{K}$, the expression of (11) will be modified to

$$\begin{aligned}\underline{\delta}_{K,\dot{K}}(\beta) &= \frac{1}{2^n}\sum_{j=1}^{m}\left|(-1)^{\beta_j}\mathcal{A}_{F_j}(K\oplus\dot{K}) + \sum_{i=1,i\neq j}^{m}(-1)^{\beta_i}\mathcal{C}_{F_i,F_j}(K\oplus\dot{K})\right| \\ &= \frac{1}{2^n}\sum_{j=1}^{m}\left|\mathcal{A}_{F_j}(K\oplus\dot{K}) + \sum_{i=1,i\neq j}^{m}(-1)^{\beta_i\oplus\beta_j}\mathcal{C}_{F_i,F_j}(K\oplus\dot{K})\right| \end{aligned} \tag{20}$$

Thus, we need to modify (16) to obtain

$$\underline{\tau}_F^{\beta} = m - \frac{1}{2^n(2^n-1)}\sum_{a\in\mathbb{F}_2^{n^*}}\sum_{j=1}^{m}\left|\mathcal{A}_{F_j}(a) + \sum_{i=1,i\neq j}^{m}(-1)^{\beta_i\oplus\beta_j}\mathcal{C}_{F_i,F_j}(a)\right|. \tag{21}$$

One may note that under this definition too, we have

$$\underline{\tau}_F^{\beta} = \underline{\tau}_F^{\overline{\beta}}. \tag{22}$$

Consequently, modifying (17), we obtain

$$\underline{\tau}_F = \max_{\beta \in \mathbb{F}_2^m} \left(m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \sum_{j=1}^{m} \left| \mathcal{A}_{F_j}(a) + \sum_{i=1, i \neq j}^{m} (-1)^{\beta_i \oplus \beta_j} \mathcal{C}_{F_i, F_j}(a) \right| \right). \tag{23}$$

Remark 1. From the designers point of view, it is important to consider the β for which $\underline{\tau}_F^{\beta}$ will be minimum. In this case, the attacker's advantage is minimum when β is in the circuit as the precharge logic value. On the other hand, if the precharge logic value is such that $\underline{\tau}_F^{\beta}$ is maximum, then that will make the attacker's advantage maximum in this model. In particular, given any precharge logic value β, the DPA should be possible and that is clearly noted through our definition.

One may note that our revised definition of TO (as well in the case of earlier definition in [13]) is invariant under the affine transformation of the S-Box. We obtained an interesting lower bound of $\underline{\tau}_F$ as presented in Appendix B in detail. The main combinatorial contribution in this bound is that, all the cross-correlation terms could be replaced by Walsh spectrum values.

4.1 Example with some existing S-boxes

Let us first refer to the 8×8 S-box F of AES [1]. The graphical representation $\underline{\tau}_F(\beta)$ is presented in Figure 3 and one may note the symmetry due to $\underline{\tau}_F^{\beta} = \underline{\tau}_F^{\overline{\beta}}$. We have noted that the minimum

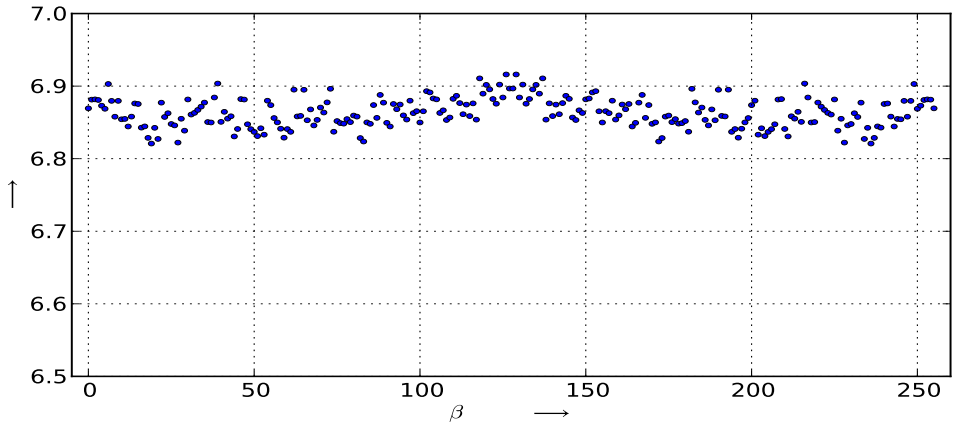

Fig. 3. Values of $\underline{\tau}_F^{\beta}$ as β varies over $\mathbb{F}_2^8$ for AES S-box. The 8-bit patterns of β are written as their integer values.

value of $\underline{\tau}_F^{\beta}$ is 6.82083 which occurs at $\beta = \beta_{\min} = (0, 0, 0, 1, 0, 0, 1, 1)$ (integer value 19) and its complement, whereas the maximum value is 6.91605 which occurs at $\beta = \beta_{\max} = (0, 1, 1, 1, 1, 1, 1, 0)$ (integer value 126) and its complement. Thus, we have $\underline{\tau}_F = 6.91605$. From the designers point

of view, it is better to use $\beta_{\min}$ as the precharge logic as in that case more effort will be required (than when any other β is the precharge logic) to identify the peak corresponding to the correct key. Our lower bound of $\underline{\tau}_F$ presented in Theorem 2 of Appendix B provides the value 6.51457. We have also analyzed the family of S-boxes in the context of Prince [3] (details in Appendix C). Our analysis shows that all the eight different 4×4 S-boxes are not of the same property in terms of the values of $\underline{\tau}_F^{\beta}$.

5 Conclusion

In this paper we have critically analysed the definition of Transparency Order (TO) as presented in [13] almost a decade back. Surprisingly, there are a few inconsistencies in the definition as well as in the interpretation of the definition that went unnoticed for such a long time. We have pointed those out in this paper. There were several implicit assumptions considered in [13] for studying the definition. While some of them were logical, the one assuming all the values in cross-correlation spectra zero under some independence condition was indeed not correct. A few correct assumptions on balancedness of component functions were made in [13], but the definition was applied to bent functions (unbalanced) in [13, 5] that lead to wrong conclusions. The definition of [13] considered maximization over all $\beta \in \mathbb{F}_2^m$, but we have proved that the maximum is automatically attained for all-zero and all-one β, making the definition of [13] redundant. Then we have made a detailed step by step analysis of DPA in Hamming weight model where the value β is considered to be constant in precharge logic implementation. We have identified all the issues that provided the redundant definition of TO in [13] and misled further research. Finally we have provided a revised definition of Transparency Order (TO) that takes care of both designers' and cryptanalysts' viewpoints. We have presented numerical data for the AES S-box and the family of S-boxes used in the context of Prince.

References

1. Advanced Encryption Standard. `http://en.wikipedia.org/wiki/Rijndael_S-box`
2. Begul Bilgin, Svetla Nikova, Ventzislav Nikov, Vincent Rijmen, Georg Stutz. Threshold Implementations of All 3×3 and 4×4 S-Boxes. CHES 2012. Lecture Notes in Computer Science, 2012, Volume 7428, pp 76-91.
3. Julia Borghoff, Anne Canteaut, Tim Guneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Soren S. Thomsen, and Tolga Yalcin. PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications - Extended Abstract. ASIACRYPT 2012. Lecture Notes in Computer Science, 2012, Volume 7658, pp 208-225. Full version of the paper at `http://eprint.iacr.org/2012/529`
4. Eric Brier, Christophe Clavier, and Francis Olivier. Correlation Power Analysis with a Leakage Model. CHES 2004. Lecture Notes in Computer Science, 2004, Volume 3156, pp 16-29.
5. Claude Carlet. On Highly Nonlinear S-Boxes and Their Inability to Thwart DPA Attacks. INDOCRYPT 2005. Lecture Notes in Computer Science, Volume 3797, 2005, pp 49-62.
6. Yunsi Fei, Qiasi Luo and A. Adam Ding. A Statistical Model for DPA with Novel Algorithmic Confusion Analysis. CHES 2012. Lecture Notes in Computer Science, 2012, Volume 7428, pp 233-250.
7. Sylvain Guilley, Philippe Hoogvorst, and Renaud Pacalet. Differential Power Analysis Model and Some Results. Proceedings of Smart Card Research and Advanced Applications VI - CARDIS 2004. Kluwer Academic Publishers, 2004, pp 127-142.
8. Annelie Heuser, Olivier Rioul and Sylvain Guilley. A Theoretical Study of Kolmogorov-Smirnov Distinguishers: Side-Channel Analysis vs. Differential Cryptanalysis. COSADE 2014.
9. Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis: Leaking Secrets. CRYPTO 1999. Lecture Notes in Computer Science, 1999, Volume 1666, pp 388-397.

10. Stefan Mangard, Norbert Pramstaller, and Elisabeth Oswald. Successfully Attacking Masked AES Hardware Implementations. CHES 2005. Lecture Notes in Computer Science, 2005, Volume 3659, pp 157-171.
11. Bodhisatwa Mazumdar, Debdeep Mukhopadhyay, and Indranil Sengupta. Constrained Search for a Class of Good Bijective S-Boxes with Improved DPA Resistivity. *IEEE Transactions on Information Forensics and Security*, 8(12):2154–2163, 2013.
12. Svetla Nikova, Vincent Rijmen, Martin Schlaffer. Secure Hardware Implementation of Nonlinear Functions in the Presence of Glitches. J. Cryptology 24(2): 292-321, 2011.
13. Emmanuel Prouff. DPA Attacks and S-Boxes. Proceedings of the Fast Software Encryption. Lecture Notes in Computer Science, Volume 3557, 2005, pp 424-441.
14. Oscar Reparaz, Benedikt Gierlichs and Ingrid Verbauwhede. A note on the use of margins to compare distinguishers. COSADE 2014.
15. Matthieu Rivain, Emmanuel Prouff. Provably Secure Higher-Order Masking of AES. CHES 2010. Lecture Notes in Computer Science, Volume 6225, 2010, pp 413-427.
16. Elena Trichina, Domenico De Seta, and Lucia Germani. Simplified Adaptive Multiplicative Masking for AES. CHES 2002. Lecture Notes in Computer Science, 2002, Volume 2523, pp 187-197.
17. Carolyn Whitnall and Elisabeth Oswald. A Comprehensive Evaluation of Mutual Information Analysis Using a Fair Evaluation Framework. CRYPTO 2011. Lecture Notes in Computer Science, 2011, Volume 6841, pp 316-334.
18. Carolyn Whitnall and Elisabeth Oswald. A Fair Evaluation Framework for Comparing Side-Channel Distinguishers. J. Cryptographic Engineering, 1(2), 2011, pp. 145-160.

Appendix A: Detailed calculations

$\Delta_{K,\dot{K}}(j,\beta)$ in terms of S-box parameters

$$\begin{aligned}\Delta_{K,\dot{K}}(j,\beta) &= -\frac{1}{2^{n-1}}\sum_{x\in\mathbb{F}_2^n}(-1)^{F_j(x\oplus K)}H\left(F(x\oplus\dot{K})\oplus\beta\right) \\ &= -\frac{1}{2^{n-1}}\sum_{x\in\mathbb{F}_2^n}(-1)^{F_j(x\oplus K)}\sum_{i=1}^{m}(F_i(x\oplus\dot{K})\oplus\beta_i) \\ &= -\frac{1}{2^{n-1}}\sum_{x\in\mathbb{F}_2^n}(-1)^{F_j(x\oplus K)}\ \frac{1}{2}\left(m-\sum_{i=1}^{m}(-1)^{F_i(x\oplus\dot{K})\oplus\beta_i}\right) \\ &= -\frac{m}{2^n}\sum_{x\in\mathbb{F}_2^n}(-1)^{F_j(x\oplus K)}+\frac{1}{2^n}\sum_{i=1}^{m}(-1)^{\beta_i}\sum_{x\in\mathbb{F}_2^n}(-1)^{F_j(x\oplus K)\oplus F_i(x\oplus\dot{K})}\end{aligned} \tag{24}$$

Calculations related to $\Delta_{K,\dot{K}}(j,\beta)$

$$\Delta_{K,\dot{K}}(j,\beta) = Q_1 + Q_2, \text{ where} \tag{25}$$

$$Q_1 = \frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{\beta_j}(-1)^{F_j(x\oplus K)\oplus F_j(x\oplus\dot{K})} = \frac{(-1)^{\beta_j}}{2^n}\mathcal{A}_{F_j}(K\oplus\dot{K}), \text{ for } i=j, \text{ and}$$

$$\begin{aligned}Q_2 &= \frac{1}{2^n}\sum_{i=1,i\neq j}^{m}(-1)^{\beta_i}\sum_{x\in\{0,1\}^n}(-1)^{F_j(x\oplus K)\oplus F_i(x\oplus\dot{K})}, \text{ for } i\neq j \\ &= \frac{1}{2^n}\sum_{i=1,i\neq j}^{m}(-1)^{\beta_i}\mathcal{C}_{F_j,F_i}(K\oplus\dot{K}).\end{aligned}$$

Proof of $\tau'^{\overline{\beta}}_F = \tau'^{\beta}_F$

$$\begin{aligned}
\tau'^{\overline{\beta}}_F &= |m - 2H(\overline{\beta})| \\
&\quad - \frac{1}{2^n(2^n-1)} \sum_{a \in \mathbb{F}_2^{n*}} \left| \sum_{j=1}^{m} \left((-1)^{\overline{\beta}_j} \mathcal{A}_{F_j}(a) + \sum_{i=1, i\neq j}^{m} (-1)^{\overline{\beta}_i} \mathcal{C}_{F_i,F_j}(a) \right) \right| \\
&= |m - 2H(\beta)| \\
&\quad - \frac{1}{2^n(2^n-1)} \sum_{a \in \mathbb{F}_2^{n*}} \left| \sum_{j=1}^{m} \left(-(-1)^{\beta_j} \mathcal{A}_{F_j}(a) - \sum_{i=1, i\neq j}^{m} (-1)^{\beta_i} \mathcal{C}_{F_i,F_j}(a) \right) \right| \\
&= |m - 2H(\beta)| \\
&\quad - \frac{1}{2^n(2^n-1)} \sum_{a \in \mathbb{F}_2^{n*}} \left| \sum_{j=1}^{m} \left((-1)^{\beta_j} \mathcal{A}_{F_j}(a) + \sum_{i=1, i\neq j}^{m} (-1)^{\beta_i} \mathcal{C}_{F_i,F_j}(a) \right) \right| \\
&= \tau'^{\beta}_F. \qquad (26)
\end{aligned}$$

Appendix B: A lower bound of $\underline{\tau}_F$ using Walsh spectrum only

We present a lower bound of $\underline{\tau}_F$ for a given $F = (F_1, \ldots, F_m)$. The following result will be used to derive the bound.

Lemma 1. *Suppose e, f, g, h are Boolean functions of n-variables. Then*

$$\sum_{a \in \mathbb{F}_2^n} \mathcal{C}_{e,f}(a)\mathcal{C}_{g,h}(a) = \frac{1}{2^n} \sum_{a \in \mathbb{F}_2^n} W_e(a)W_f(a)W_g(a)W_h(a).$$

Proof. Suppose $\mathbb{F}_2^n = \{a_0, \ldots, a_{2^n-1}\}$. It is known that

$$[\mathcal{C}_{e,f}(a_0), \ldots, \mathcal{C}_{e,f}(a_{2^n-1})]\mathcal{H}_n = [W_e(a_0)W_f(a_0), \ldots, W_e(a_{2^n-1})W_f(a_{2^n-1})]$$

$$[\mathcal{C}_{g,h}(a_0), \ldots, \mathcal{C}_{g,h}(a_{2^n-1})]\mathcal{H}_n = [W_g(a_0)W_h(a_0), \ldots, W_g(a_{2^n-1})W_h(a_{2^n-1})],$$

where $\mathcal{H}_n$ is the Hadamard matrix of order $2^n \times 2^n$. Take the product

$$\begin{aligned}
&[\mathcal{C}_{e,f}(a_0), \ldots, \mathcal{C}_{e,f}(a_{2^n-1})]\mathcal{H}_n \Big([\mathcal{C}_{g,h}(a_0), \ldots, \mathcal{C}_{g,h}(a_{2^n-1})]\mathcal{H}_n \Big)^T \\
&= [W_e(a_0)W_f(a_0), \ldots, W_e(a_{2^n-1})W_f(a_{2^n-1})] \begin{pmatrix} W_g(a_0)W_h(a_0 \\ \vdots \\ W_g(a_{2^n-1})W_h(a_{2^n-1}) \end{pmatrix}
\end{aligned}$$

Since, $\mathcal{H}_n\mathcal{H}_n^T = 2^n I_{2^n \times 2^n}$, where $I_{2^n \times 2^n}$ is the identity matrix of order $2^n \times 2^n$, then from the product, we have

$$\sum_{a \in \mathbb{F}_2^n} \mathcal{C}_{e,f}(a)\mathcal{C}_{g,h}(a) = \frac{1}{2^n} \sum_{a \in \mathbb{F}_2^n} W_e(a)W_f(a)W_g(a)W_h(a).$$

Theorem 2. *For $F = (F_1, \ldots, F_m) : \mathbb{F}_2^n \to \mathbb{F}_2^m$, the value of $\underline{\tau}_F$ has the following lower bound*

$$m - \frac{\sqrt{2^n-1}}{(2^{2n}-2^n)} \sum_{j=1}^{m} \Bigg(\sum_{i=1}^{m} \sum_{a \in F_2^{n*}} W_{F_i}^2(a) W_{F_j}^2(a) + 2 \sum_{1 \le i < k \le m} \sum_{a \in F_2^{n*}} W_{F_i}(a) W_{F_j}^2(a) W_{F_k}(a) \Bigg)^{\frac{1}{2}}.$$

Proof. It is clear that $\underline{\tau}_F \geq \underline{\tau}_F^0$. So we calculate a lower bound of $\underline{\tau}_F^0$. From (21) we get

$$\underline{\tau}_F^0 = m - \frac{1}{(2^{2n}-2^n)} \sum_{j=1}^{m} \sum_{a \in F_2^{n*}} |\mathcal{A}_{F_j}(a) + \sum_{\substack{i=1 \\ i \neq j}}^{m} \mathcal{C}_{F_i,F_j}(a)| \tag{27}$$

Applying Cauchy-Schwarz inequality we get

$$\begin{aligned} \sum_{a \in F_2^{n*}} |\sum_{i=1}^{m} \mathcal{C}_{F_i,F_j}(a)| &\leq \Bigg((2^n-1) \sum_{a \in F_2^{n*}} \Big(\sum_{i=1}^{m} \mathcal{C}_{F_i,F_j}(a) \Big)^2 \Bigg)^{\frac{1}{2}} \\ &= \Bigg((2^n-1) \sum_{a \in F_2^{n}} \Bigg[\Big(\sum_{i=1}^{m} \mathcal{C}_{F_i,F_j}(a) \Big)^2 - \Big(\sum_{i=1}^{m} \mathcal{C}_{F_i,F_j}(0) \Big)^2 \Bigg] \Bigg)^{\frac{1}{2}} \\ &= \Bigg((2^n-1) \sum_{a \in F_2^{n}} \Big(\sum_{i=1}^{m} \mathcal{C}_{F_i,F_j}(a) \Big)^2 \Bigg)^{\frac{1}{2}} \end{aligned} \tag{28}$$

Note that

$$\begin{aligned} \sum_{a \in F_2^n} \Big(\sum_{i=1}^{m} \mathcal{C}_{F_i,F_j}(a) \Big)^2 &= \sum_{a \in F_2^n} \sum_{i=1}^{m} \mathcal{C}_{F_i,F_j}^2(a) + 2 \sum_{a \in F_2^n} \sum_{1 \le i < k \le m} \mathcal{C}_{F_i,F_j}(a) \mathcal{C}_{F_k,F_j}(a) \\ &= \sum_{i=1}^{m} \sum_{a \in F_2^n} \mathcal{C}_{F_i,F_j}^2(a) + 2 \sum_{1 \le i < k \le m} \sum_{a \in F_2^n} \mathcal{C}_{F_i,F_j}(a) \mathcal{C}_{F_k,F_j}(a) \end{aligned}$$

Then applying Lemma 1,

$$\sum_{a \in F_2^n} \Big(\sum_{i=1}^{m} \mathcal{C}_{F_i,F_j}(a) \Big)^2 = \sum_{i=1}^{m} \sum_{a \in F_2^n} W_{F_i}^2(a) W_{F_j}^2(a) + 2 \sum_{1 \le i < k \le m} \sum_{a \in F_2^n} W_{F_i}(a) W_{F_j}^2(a) W_{F_k}(a).$$

Replacing this value of $\sum_{a \in F_2^n} \Big(\sum_{i=1}^{m} \mathcal{C}_{F_i,F_j}(a) \Big)^2$ in (28), an upper bound of $\sum_{a \in F_2^{n*}} |\sum_{i=1}^{m} \mathcal{C}_{F_i,F_j}(a)|$ is obtained. Then using this upper bound in (27), we get a lower bound of $\underline{\tau}_F^0$ as follows

$$m - \frac{\sqrt{2^n-1}}{(2^{2n}-2^n)} \sum_{j=1}^{m} \Bigg(\sum_{i=1}^{m} \sum_{a \in F_2^{n}} W_{F_i}^2(a) W_{F_j}^2(a) + 2 \sum_{1 \le i < k \le m} \sum_{a \in F_2^{n}} W_{F_i}(a) W_{F_j}^2(a) W_{F_k}(a) \Bigg)^{\frac{1}{2}}.$$

Note that $\underline{\tau}_F^{\beta}$ assumes that all the coordinate functions are balanced, therefore the above bound can be written as

$$m - \frac{\sqrt{2^n-1}}{(2^{2n}-2^n)} \sum_{j=1}^{m} \Bigg(\sum_{i=1}^{m} \sum_{a \in F_2^{n*}} W_{F_i}^2(a) W_{F_j}^2(a) + 2 \sum_{1 \le i < k \le m} \sum_{a \in F_2^{n*}} W_{F_i}(a) W_{F_j}^2(a) W_{F_k}(a) \Bigg)^{\frac{1}{2}}.$$

This serves as a lower bound of $\underline{\tau}_F$. □

Appendix C: Analysis for the S-boxes in context of Prince

Eight 4×4 S-boxes are referred in [3]. In Table 1 we show the maximum and minimum values of $\underline{\tau}_F^{\beta}$ for each of the S-boxes.

S-Box	$\beta_{\max}$ (as integer)	$\max_{\beta \in \mathbb{F}_2^4} \underline{\tau}_F^{\beta}$	$\beta_{\min}$ (as integer)	$\min_{\beta \in \mathbb{F}_2^4} \underline{\tau}_F^{\beta}$
S-box-1	0	2.46667	1	1.63333
S-box-2	2	2.56666	1	1.7
S-box-3	2	2.53333	1	1.66667
S-box-4	4	2.46667	1	1.56667
S-box-5	4	2.53333	2	2.16667
S-box-6	0	2.46667	6	2.1
S-box-7	6	2.5	5	2.23333
S-box-8	2	2.66667	7	2.2

Table 1. Maximum (corresponding to $\beta_{\max}$) and minimum (corresponding to $\beta_{\min}$) values of $\underline{\tau}_F^{\beta}$ as β varies over $\mathbb{F}_2^4$ for the eight Prince S-boxes (available in Table 3 of Appendix C in the eprint version of [3]).

The complete graphical representation for the eight S-boxes are presented next in Figure 4.

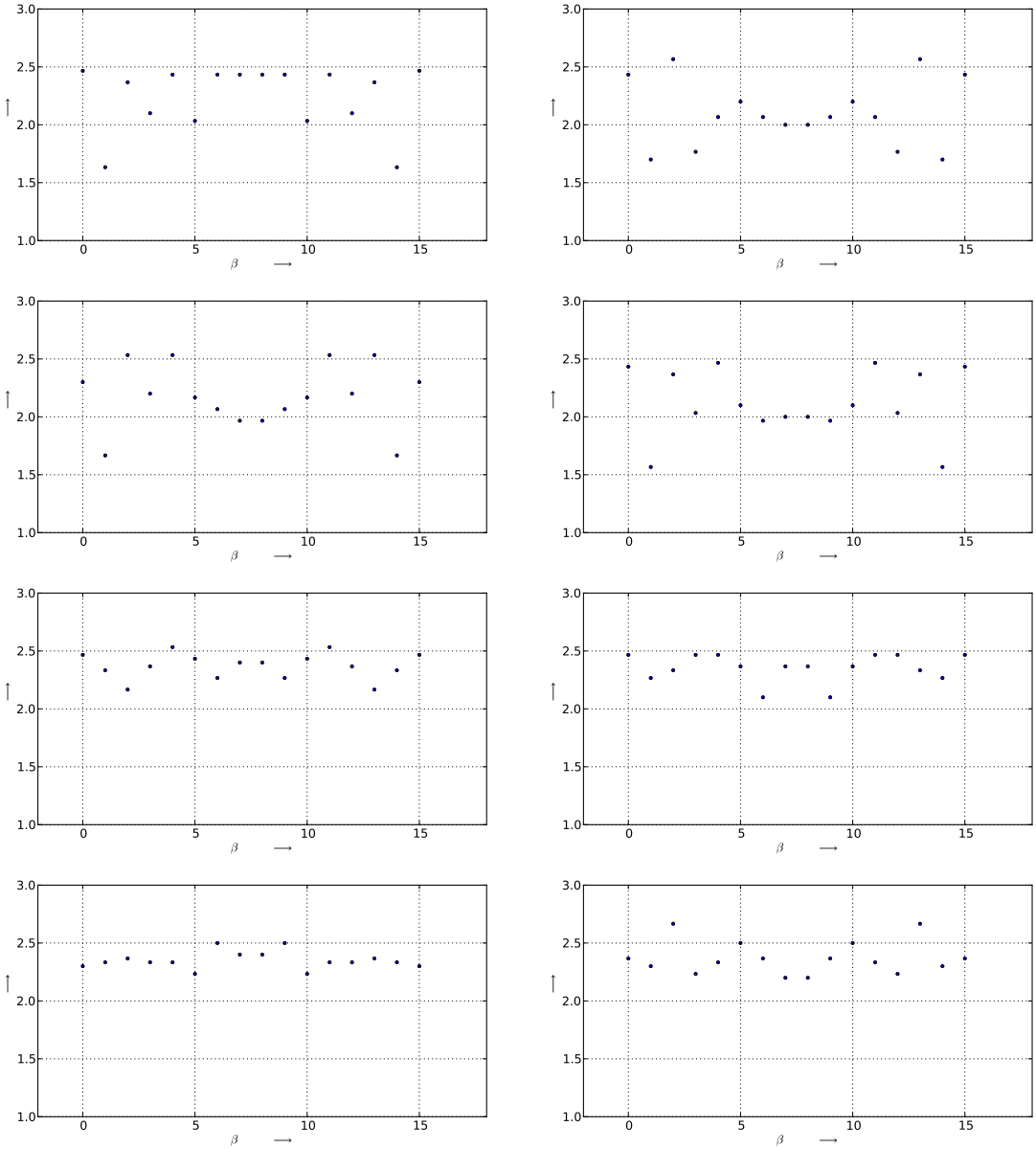

Fig. 4. Values of $\underline{\tau}_F^{\beta}$ as β varies over $\mathbb{F}_2^4$ for the Prince S-boxes