Redefining the Transparency Order

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

Redefining the Transparency Order ⋆

Kaushik Chakraborty[1], Sumanta Sarkar[2], Subhamoy Maitra[2], Bodhisatwa Mazumdar[3], Debdeep Mukhopadhyay[3], and Emmanuel Prouff[4]

[1] SECRET Team, INRIA, Rocquencourt
kaushik.chakraborty@inria.fr
[2] Indian Statistical Institute, Kolkata
sumanta.sarkar@gmail.com, subho@isical.ac.in
[3] Indian Institute of Technology, Kharagpur
bm.iitkgp@gmail.com, debdeep.mukhopadhyay@gmail.com
[4] Agence nationale de la scurit des systmes d'information (ANSSI)
e.prouff@gmail.com

Abstract. In this paper, we revisit the definition of Transparency Order (TO) from the work of Prouff (FSE 2005) that was proposed to measure the resistance of an s-box against Differential Power Analysis. We 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. We analyze the definition from scratch, modify it and finally provide a revised definition. Our simulation results confirm that the transparency order is indeed related to the resistance of the s-box against side-channel attacks. Thus (revised) TO is one of the valuable criteria to consider when designing a cryptographic algorithm.

Keywords: AES, Cross-correlation, Differential Power Analysis, PRINCE, s-box, Transparency Order.

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 being executed on a cryptographic platform. To resist such attacks, algorithmic countermeasures like masking [7] and leakage resistant logic [17] exist, that may lead to increased footprint on the implementation platforms in terms of area and power consumptions. Because of phenomenon like glitches, it should be noted that in practical scenarios even masked circuits can be subjected to DPA. 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

⋆ An extended version with greater details of our contributions is available in [5].

linear and differential cryptanalysis. An attempt to quantify the DPA resilience of the s-boxes was made in [15], where the parameter Transparency Order (TO) was introduced, with the implication that s-boxes with smaller TO have higher DPA resilience. Further analyses of TO, as defined in [15], have been followed in *e.g.,* [4, 12].

In this paper, we exhibit several inconsistencies in the original definition given in [15] that has been unnoticed over a decade, and we provide an improved definition of the transparency order that appears to be a better metric for quantifying the resistance of an s-box to DPA attacks. Eventually, its soundness to quantify the resistance of an s-box against side-channel attacks is investigated thanks to several attack simulations.

2 Preliminaries

2.1 Basics of Boolean functions

Let $\mathbb{F}_2^n$ be the vector space that contains all the n-bit binary vectors. The *Hamming weight* denoted by $\mathsf{H}(u)$ is the number of 1's in the binary vector $u \in \mathbb{F}_2^n$. A Boolean function on n variables is a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. . The support of a Boolean function f is defined as $Supp(f) = \{x \in \mathbb{F}_2^n | f(x) = 1\}$, when $|Supp(f)| = 2^{n-1}$, then f is called *balanced* function. The *autocorrelation transform* of $f(x)$ is an integer valued function over $\mathbb{F}_2^n$ which is defined as $\mathcal{A}_f(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus \omega)}$. On the other hand *cross-correlation coefficient* between two Boolean functions; for f_1, f_2, it is defined for every $\omega \in \mathbb{F}_2^n$ as the value $\mathcal{C}_{f_1,f_2}(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f_1(x) \oplus f_2(x \oplus \omega)}$ (note that we have $\mathcal{C}_{f,f}(\omega) = \mathcal{A}_f(\omega)$). An $n \times m$ s-box F can be seen as a multi-output Boolean function, namely a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$ with $m \leq n$.

2.2 DPA Attack and Transparency Order of s-boxes

Differential Power Analysis (DPA) introduced by Kocher et al [10], 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. It consists in observing the processing of a cryptographic algorithm (*e.g.,* a block cipher) and in measuring a sample of power consumption traces $\boldsymbol{T}_x$ related to a sufficiently large number of plaintexts x. Next, based on these power traces, the actual attack can be mounted off-line to get the information about the secret key.

Single-bit DPA attack works in the following way: let j denote the index of the targeted bit and let $\dot{K}$ denote a secret sub-part that statistically depends on this bit (assuming that the block cipher is iterative, $\dot{K}$ may correspond to the secret parameter of an s-box and is typically 4, 6 or 8 bit long). The attacker makes a guess K on $\dot{K}$ and then the traces are assigned in either of the two bins, say S_0 and S_1, according to hypotheses on the targeted bit which are deduced from K and the plaintexts x. To discriminate the good guess from

the wrong ones, [10] proposes to compute the *differential trace* $\boldsymbol{D}_{K,j}$ defined by $\boldsymbol{D}_{K,j} = \frac{1}{|S_1|}\sum_{\boldsymbol{T}_x \in S_1} \boldsymbol{T}_x - \frac{1}{|S_0|}\sum_{\boldsymbol{T}_x \in S_0} \boldsymbol{T}_x$. The quantity $\boldsymbol{D}_{K,j}$ works as a distinguisher in the single-bit power attack model. According to the theory proposed in [10] the vector $\boldsymbol{D}_{K,j}$ should show a peak for the correct key $K = \dot{K}$. Single-bit DPA attack was extended to the *multi-bit DPA* introduced by Messerges in [13], which is called *multi-bit DPA*.

In [9], a few ideas were presented to measure the efficiency of DPA on an s-box in the Hamming distance model with independent additive noise [3]. This model assumes that the leakage takes the form $\mathsf{H}(\beta \oplus F(x \oplus \dot{K})) + B$, where x and $\dot{K}$ respectively denote a plaintext and a round key sub-part, where β denotes the initial content of the register before updating with $F(x \oplus \dot{K})$ and where B denotes an independent (measurement) noise. The idea of [9] has been afterwards extended in [15] to encompass multi-bit DPA, and introduced the notion of *transparency order* (TO) to quantify the resistance of s-boxes against DPA attacks. Lower the TO value, better the resistance against DPA. The TO notion introduced in [15] not only depends on the s-box's algebraic properties but also on the register's initial state $\beta \in \mathbb{F}_2^m$ which is assumed to be constant for some platforms like smart cards which are based on *precharge logic*. After certain assumptions, the final formula defining the TO of a $n \times m$ s-box $F = (F_1, \ldots, F_m)$ is given by:

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

3 Redundant Definition of Transparency Order [15]

In this section, we explain why the definition (1) is redundant. For such a purpose, we take $\tau_F^\beta = |m - 2\mathsf{H}(\beta)| - \frac{1}{2^{2n}-2^n}\sum_{a \in \mathbb{F}_2^{n*}} |\sum_{i=1}^{m} (-1)^{\beta_i} \mathcal{A}_{F_i}(a)|$ in (1) and $\nu_{F,\beta} = \frac{1}{2^{2n}-2^n}\sum_{\alpha \in \mathbb{F}_2^{n*}} |\sum_{i=1}^{m} (-1)^{\beta_i} \mathcal{A}_{F_i}(\alpha)|$. With these new notations, we have $\mathsf{TO}(F) = \max_{\beta \in \mathbb{F}_2^m} \tau_F^\beta$. We give hereafter our first result.

Proposition 1. $\tau_F^\beta = \tau_F^{\overline{\beta}}$.

Next we present the most important result of this section.

Proposition 2. *Let* $0 < \mathsf{H}(\beta) \leq \lfloor \frac{m}{2} \rfloor$. *Then* $\tau_F^\beta \leq \tau_F^{\mathbf{0}}$.

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

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

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

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,

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

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

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

4 Critically analyzing TO for Multi-bit DPA Attack

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 $\mathsf{H}(F(x \oplus \dot{K}) \oplus \beta)$. The basic idea of DPA works as follows.

Let us concentrate on the j-th output bit of the s-box. Given any key K (which may or may not be the correct key $\dot{K}$), we put the power related information in two bins depending on the value of $F_j(x \oplus K)$. As in [15], 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

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

where $S_{K,0} = \{x | F_j(x \oplus K) = 0\}$ and $S_{K,1} = \{x | F_j(x \oplus K) = 1\}$.

Note that most of the practical s-boxes are balanced, *i.e.,* every coordinate function F_j is balanced, as well as every component functions of the form $F_i \oplus F_j$

is balanced. [15] too considered balanced s-boxes, and for a balanced s-box F we have

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

In single-bit DPA attack the expression $\Delta_{K,\dot{K}}(j,\beta)$ is calculated for a fixed index j and for all hypotheses $K \in \mathbb{F}_2^n$. In the multi-bit case, the latter calculation is done for every $j \in [1..m]$. This actually leads to the processing of the following quantity $\delta_{K,\dot{K}}(\beta)$ [15, Equation (10)]:

$$\delta_{K,\dot{K}}(\beta) = |\sum_{j=1}^{m}\Delta_{K,\dot{K}}(j,\beta)|. \quad (3)$$

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

$$\delta_{K,\dot{K}}(\beta) = \frac{1}{2^n}\left|\sum_{j=1}^{m}\sum_{i=1}^{m}(-1)^{\beta_i}\mathcal{C}_{F_i,F_j}(K\oplus\dot{K})\right| \quad . \quad (4)$$

And, for $K = \dot{K}$, we have:

$$\delta_{\dot{K},\dot{K}}(\beta) = \left|\sum_{j=1}^{m}(-1)^{\beta_j}\left(1+\frac{1}{2^n}\sum_{i=1,i\neq j}^{m}(-1)^{\beta_i\oplus\beta_j}\mathcal{C}_{F_i,F_j}(0)\right)\right| \quad , \quad (5)$$

and we also have $\delta_{\dot{K},\dot{K}}(\beta) = \left|\sum_{j=1}^{m}(-1)^{\beta_j}\right| = |m - 2\mathsf{H}(\beta)|$. Then [15] considered

$$\mathsf{TO}(F) = \max_{\beta\in\mathbb{F}_2^m}\tau_F^\beta, \text{ where } \tau_F^\beta = \frac{1}{2^n-1}\sum_{K\in F_2^n\setminus\{\dot{K}\}}\left(\delta_{\dot{K},\dot{K}}(\beta) - \delta_{K,\dot{K}}(\beta)\right) \quad . \quad (6)$$

[15] further made a strong assumption: The cross-correlation terms $\mathcal{C}_{F_i,F_j}(K\oplus\dot{K})$ can be considered to be zero for every $i \neq j$ and every $(K,\dot{K})$. For a balanced s-box and with this assumption, $\mathsf{TO}(F)$ takes the form of (1).

Clearly, this assumption is not true as we cannot have all the values zero in cross-correlation spectrum in general.

5 Redefining TO: considering cross correlation terms and modifying $\delta_{K,\dot{K}}(\beta)$

We already have discussed that we must consider the cross correlations terms in $\Delta_{K,\dot{K}}(j,\beta)$, however that still does not remove the redundancy in the modified definition of TO . So we also redefine $\delta_{K,\dot{K}}(\beta)$ and propose $\underline{\delta}_{K,\dot{K}}(\beta)$:

$$\underline{\delta}_{K,\dot{K}}(\beta) = \sum_{j=1}^{m}|\Delta_{K,\dot{K}}(j,\beta)| \quad . \quad (7)$$

For balanced s-box, and for $K \neq \dot{K}$, Equation (4) becomes:

$$\underline{\delta}_{K,\dot{K}}(\beta) = \frac{1}{2^n} \sum_{j=1}^{m} \left| \sum_{i=1}^{m} (-1)^{\beta_i \oplus \beta_j} \mathcal{C}_{F_i,F_j}(K \oplus \dot{K}) \right| \quad , \tag{8}$$

which leads to the following new version, called $\mathsf{TO}(F, \beta)$,

$$\mathsf{TO}(F, \beta) = m - \frac{1}{2^n(2^n-1)} \sum_{a \in \mathbb{F}_2^{n*}} \sum_{j=1}^{m} \left| \sum_{i=1}^{m} (-1)^{\beta_i \oplus \beta_j} \mathcal{C}_{F_i,F_j}(a) \right| \quad , \tag{9}$$

where $a = K \oplus \dot{K}$ in (8).

Remark 1. We still have $\mathsf{TO}(F, \beta) = \mathsf{TO}(F, \overline{\beta})$.

We eventually deduce the following new definition of the TO criterion:

Definition 1 (Improved Transparency Order). *Let F be a balanced $n \times m$ function. Its improved transparency order is the coefficient $\mathsf{TO}(F)$ defined by:*

$$\mathsf{TO}(F) = \max_{\beta \in \mathbb{F}_2^m} \left(m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \sum_{j=1}^{m} \left| \sum_{i=1}^{m} (-1)^{\beta_i \oplus \beta_j} \mathcal{C}_{F_i,F_j}(a) \right| \right) \quad . \tag{10}$$

For the 8×8 s-box (the inverse function) used in `AES` [8], the minimum value of $\mathsf{TO}(F, \beta)$ is 6.82083 which is at $\beta = \beta_{\min} = (0, 0, 0, 1, 0, 0, 1, 1)$ and its complement, whereas the maximum value 6.91605 is achieved at $\beta_{\max} = (0, 1, 1, 1, 1, 1, 1, 0)$ and its complement. Thus We hence deduce that the TO of the `AES` s-box is $\mathsf{TO}(F) = 6.91605$. Needless to say these values are different from TO as proposed in [15]. In Table 1, we present $\mathsf{TO}(F)$ values for eight 4×4 s-boxes belong to PRINCE [2].

s-box	$\beta_{\max}$ (as integer)	$\mathsf{TO}(F)$	$\beta_{\min}$ (as integer)	$\mathsf{TO}_{\min}(F)$
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 $\mathsf{TO}(F, \beta)$ as β varies over $\mathbb{F}_2^4$ for the eight `PRINCE` s-boxes.

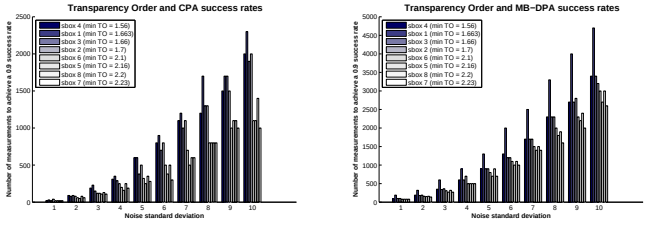
6 Practical Soundness of the Transparency Order

6.1 Attack Simulations

This section aims to confront the notion of (revised) transparency order with attack simulations. Essentially, our goal is to study to what extent the low trans-

parency order of an s-box impacts the efficiency of a side channel attack against its processing.

We first performed CPA attack simulations against the 8 PRINCE s-boxes listed in Table 1. We think that the latter ones are good targets for our study since their minimum transparency order are reasonably different and ranges from 1.56667 (for s-box 4) to 2.23333 (for s-box 7). In these first tests campaign, we choose to simulate the information leakage in the classical Hamming Distance model with Gaussian noise. Namely, the leakage $L(X \oplus \dot{K})$ related to the processing of the s-box output $F(X + \dot{K})$ equals $\mathsf{H}(F(x \oplus \dot{K}) \oplus \beta) + B$, where B is a random variable whose distribution is Gaussian with null mean and standard deviation σ. The value β corresponds to the initial state of the memory before the writing of $F(x \oplus \dot{K})$. According to the discussion in previous sections, we assumed that it can be chosen by the designer and, for each PRINCE s-box F, we selected it to minimize $\mathsf{TO}(F, \beta)$ (see Table 1)[5]. Each hypothesis K on $\dot{K}$ has been tested by estimating the correlation coefficient It can be noticed that the initial content β of the register is assumed to be known by the attacker, which makes sense since it is part of the design parameters and therefore must be public according to Kerckhoff's rule. The number of leakage observations used to estimate the correlation is denoted by N. Attacks have been tested for different amounts of noise (namely for different standard deviations $\sigma \in [1..10]$). For each of them, we estimated the minimum number of observations N required for the attack to succeed with a probability at least equal to 0.9. As argued in [11], this is a sound way to evaluate the efficiency of a side-channel attack. Results are reported in Figure 1(a).



(a) CPA (b) MB-DPA

Fig. 1. Minimum number of Messages (in y-axis) required to achieve a 90% success rate *versus* the noise standard deviation (in x-axis)

It may be checked in Figure 1(a) that the transparency order impacts the CPA attack efficiency in the Hamming distance model. This impact increases with the noise and, for $\sigma = 10$, the attack efficiency (*i.e.,* the number of traces) is almost multiplied by 2.5 if we compare s-boxes 1 and 7. One can also observe

[5] this should correspond to a maximum level of security.

that $\mathsf{TO}_{\min}$ alone does not fully capture the resistance against CPA since sbox 1 seems to be always more resistant than sbox 4 whereas its $\mathsf{TO}_{\min}$ is slightly greater (1.663 *versus* 1.56).

In Section 5, we related the new notion of transparency to the multi-bit DPA attack introduced in [1]. Since the latter attack is not equivalent to a CPA, we ran a second attacks simulation campaign. The results are reported in Figure 1(b). As expected, they essentially confirm the results we had with the CPA: the lower $\mathsf{TO}_{\min}(F)$, the higher the resistance against the attacks.

In the second phase of our simulations, we wanted to investigate the robustness of the transparency order criterion against stochastic errors. In other words, we studied the impact of an erroneous modelling on the s-box CPA resistance, by performing CPA attack simulations against the fourth and the seventh PRINCE s-boxes[6] under the assumption that the information is not leaking in the Hamming distance model but in an erroneous version of it. Namely, for a fixed *stochastic error* standard deviation σ_{er} chosen[7] in $\{0, 0.2, 0.4, 0.6, 0.8, 1.0\}$, we simulated the leakage $L(X \oplus \dot{K})$ such that:

$$L(X \oplus \dot{K}) = \varphi(F(X \oplus \dot{K}) \oplus \beta) + B \ , \tag{11}$$

where φ is a function defined for every $y \in \mathbb{F}_2^4$ by $\varphi(y) = \mathrm{HW}(y) + \varepsilon$ with ε randomly generated according to a normal distribution with mean 0 and standard deviation σ_{er}. The variable B still refers to an independent Gaussian noise with 0 mean and standard deviation σ. For the processing of the predictions, we kept the Hamming weight model (the adversary is not assumed to know the erroneous leakage model). The results of our CPA attack simulations are reported in Figure 2 (bins in dark blue correspond to s-box 4 whereas those in light blue correspond to s-box 7, for each standard deviation σ – in x-axis – there is one bin for each stochastic error σ_{er} in $\{0.0, 0.2, 0.4, 0.6, 0.8, 1.0\}$).

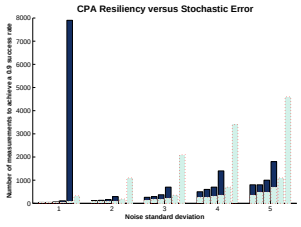


Fig. 2. CPA in presence of stochastic error - Minimum number of Messages (in y-axis) required to achieve a 90% success rate *versus* the noise standard deviation (in x-axis)

[6] those s-boxes correspond to the two opposite extrema in terms of $\mathsf{TO}_{\min}(F)$.

[7] These standard deviations correspond to j% of the mean $\mathsf{H}(y)$ when y ranges uniformly over $\mathbb{F}_2^4$ and $j \in \{0, 10, 20, 30, 40, 50\}$.

It may be checked that the fourth s-box, which has minimum $\mathsf{TO}_{\min}(F)$, stays more resistant than the seventh s-box for any stochastic error and the noise standard deviation. More interestingly, our simulations show that the difficulty of attacking s-box 4 increases more quickly with the stochastic error than for s-box 7. Actually, for a stochastic error greater than or equal to 0.8, a 90% success rate was achieved against s-box 4 only when the noise standard deviation was equal to 1. For greater noise standard deviations (and for $\sigma_{er} \geq 0.8$), this success rate was never achieved by CPA attacks with less than 500 000 traces.

7 Conclusions

In this paper we have critically analyzed the definition of transparency order originally introduced in [15]. We have exhibited several inconsistencies in the definition as well as in the interpretation of the definition that went unnoticed for a long time. Through our analysis we have revised the definition and shown the practical soundness the revised definition.

As shown by our simulations, the (minimum) transparency order is indeed related to the resistance of the s-box implementation against side channel attacks like the CPA or the multi-bit DPA. Choosing s-box with the minimum transparency order and using precharge value β for which the minimum is achieved seems therefore a good defense strategy. From this point of view, our simulations confirm our theoretical analysis. However, our simulations also show that a small minimum transparency order is not sufficient alone to achieve a satisfying resistance level against CPA: in the most favourable situation (Figure 1(a), no stochastic error and a great amount of noise), the number of needed observations to attack the s-box output is "only" multiplied by 2.5 when considering the two extreme cases of s-boxes 1 and 7. This is definitely not sufficient in practice where one usually expects that no attack succeeds with less than 1 million observations (or even more). As a conclusion, choosing s-boxes with small minimum transparency order is a good strategy if it is combined with other classical countermeasures like *e.g.,* masking [6], shuffling [16] or threshold implementation [14].

We have also noted that the (revised) TO is not invariant for affine equivalent s-boxes. Detailed results on this will appear in the full version of the paper.

Acknowledgments: This work has been partially supported by Centre of Excellence in Cryptology, Indian Statistical Institute. Kaushik Chakraborty did this work during his association with Indian Statistical Institute.

References

1. R. Bévan and E. Knudsen. Ways to Enhance Power Analysis. In P. Lee and C. Lim, editors, *Information Security and Cryptology – ICISC 2002*, volume 2587 of *Lecture Notes in Computer Science*, pages 327–342. Springer, 2002.

2. J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. S. Thomsen, and T. Yalçin. PRINCE - A low-latency block cipher for pervasive computing applications - extended abstract. In X. Wang and K. Sako, editors, *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, volume 7658 of *Lecture Notes in Computer Science*, pages 208–225. Springer, 2012.
3. E. Brier, C. Clavier, and F. Olivier. Correlation Power Analysis with a Leakage Model. In M. Joye and J.-J. Quisquater, editors, *Cryptographic Hardware and Embedded Systems – CHES 2004*, volume 3156 of *Lecture Notes in Computer Science*, pages 16–29. Springer, 2004.
4. C. Carlet. On Highly Nonlinear S-boxes and Their Inability to Thwart DPA Attacks. In S. Maitra, C. E. Veni Madhavan, and R. Venkatesan, editors, *Progress in Cryptology – INDOCRYPT 2005*, volume 3797 of *Lecture Notes in Computer Science*, pages 49–62. Springer, 2006.
5. K. Chakraborty, S. Sarkar, S. Maitra, B. Mazumdar, D. Mukhopadhyay, and E. Prouff. Redefining the transparency order. Cryptology ePrint Archive, Report 2014/367, 2014. `http://eprint.iacr.org/`.
6. S. Chari, C. Jutla, J. Rao, and P. Rohatgi. A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards. In *Second AES Candidate Conference – AES 2*, Mar. 1999.
7. S. Chari, C. Jutla, J. Rao, and P. Rohatgi. Towards Sound Approaches to Counteract Power-Analysis Attacks. In Wiener [18], pages 398–412.
8. FIPS PUB 197. *Advanced Encryption Standard*. National Institute of Standards and Technology, Nov. 2001.
9. S. Guilley, P. Hoogvorst, and R. Pacalet. Differential Power Analysis Model and Some Results. In J.-J. Quisquater, P. Paradinas, Y. Deswarte, and A. E. Kalam, editors, *Smart Card Research and Advanced Applications VI – CARDIS 2004*, pages 127–142. Kluwer Academic Publishers, 2004.
10. P. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In Wiener [18], pages 388–397.
11. S. Mangard. Hardware Countermeasures against DPA – A Statistical Analysis of Their Effectiveness. In T. Okamoto, editor, *Topics in Cryptology – CT-RSA 2004*, volume 2964 of *Lecture Notes in Computer Science*, pages 222–235. Springer, 2004.
12. B. Mazumdar, D. Mukhopadhyay, and I. 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.
13. T. Messerges. *Power Analysis Attacks and Countermeasures for Cryptographic Algorithms*. PhD thesis, University of Illinois, 2000.
14. S. Nikova, V. Rijmen, and M. Schläffer. Secure hardware implementation of nonlinear functions in the presence of glitches. *J. Cryptology*, 24(2):292–321, 2011.
15. E. Prouff. DPA attacks and S-Boxes. In H. Handschuh and H. Gilbert, editors, *Fast Software Encryption – FSE 2005*, volume 3557 of *Lecture Notes in Computer Science*, pages 424–442. Springer, 2005.
16. M. Rivain, E. Prouff, and J. Doget. Higher-Order Masking and Shuffling for Software Implementations of Block Ciphers. In C. Clavier and K. Gaj, editors, *CHES*, volume 5747 of *Lecture Notes in Computer Science*, pages 171–188. Springer, 2009.
17. K. Tiri and I. Verbauwhede. A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation. In *2004 Design, Automation and Test*

in Europe Conference and Exposition (DATE 2004), 16-20 February 2004, Paris, France, pages 246–251. IEEE Computer Society, 2004.
18. M. Wiener, editor. *Advances in Cryptology – CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*. Springer, 1999.