Modified Transparency Order Property: Solution or Just Another Attempt

Stjepan Picek^{1,2}, Bodhisatwa Mazumdar³,
Debdeep Mukhopadhyay⁴, and Lejla Batina^{2,5}

¹ Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia

² ICIS - Digital Security Group, Radboud University Nijmegen, The Netherlands

³ New York University Abu Dhabi, Abu Dhabi

⁴ Department of Computer Science and Engineering,
IIT Kharagpur, Kharagpur, India

⁵ ESAT/COSIC, KU Leuven, Belgium

Abstract. S-boxes are usual targets of side-channel attacks and it is an open problem to develop design techniques for S-boxes with improved DPA resistance. One result along that line is the transparency order, a property that attempts to characterize the resilience of S-boxes against DPA attacks. Recently, it was shown there exist flaws with the original definition of transparency, which resulted in the new definition - modified transparency order. This paper develops techniques for constructions using the modified transparency as a guiding metric. For the 4×4 size, we significantly improve modified transparency order while remaining in the optimal classes. Experimental results are provided assuming a noisy HW leakage model to show the proposed S-boxes are more resistant than the original one of the PRESENT algorithm. We conclude with reports on 4×4 and 8×8 S-boxes where the results indicate that the modified transparency order could be a more useful metric than the transparency order. However, both measures are far from definitive solution on how to improve the DPA resistance.

Keywords: S-box, Modified transparency order, DPA-resilience, Lightweight cryptography.

1 Introduction

When discussing the security of modern block ciphers, it is often natural to discuss it through the prism of resilience against certain cryptographic attacks. Alongside differential [1] and linear [2] cryptanalysis, it is expected today that the algorithm possesses resistance also against side-channel attacks [3]. In order to defend against the first two types of cryptanalysis, Substitution Boxes (S-boxes) play a significant role. In fact, in many block ciphers, S-box is the only nonlinear part and therefore fundamental for the security of a whole cipher [4]. Somewhat surprising, in recent years researchers found that S-boxes have inherent resistance against side-channel analysis (SCA) (some more and some less). Naturally, there

exist numerous countermeasures such as various hiding and masking schemes that improve the algorithm resiliency to SCA [5].

First property that connected S-boxes and their resistance against side-channel attacks was SNR (DPA) [6]. Next, Prouff introduced transparency order [7], a property that characterizes the resistance of S-boxes to the SCA or more precisely to differential power analysis (DPA) [8]. Later, Fei introduced confusion coefficient where it is possible to separate the target device, the number of traces and the algorithm under the examination [9–12]. Up to now, transparency order received the most interest so we can speak about a whole line of research about the transparency order property as it is detailed below in Section 1.1.

Recently, Chakraborty et al. showed that the original transparency order definition is flawed and they proposed amendments to it that resulted in the modified transparency order property. However, until now, there has been no practical examination of this new property.

In accordance with that, in this paper we concentrate on generating S-boxes that have good values of modified transparency order property. By good values, we mean such values that are better than those found in currently used S-boxes.

When generating S-boxes we concentrate on the two most widely used S-box sizes; more precisely, 4×4 and 8×8 . The first one is used in lightweight cryptographic algorithms like PRESENT [13] or PRINCE [14] while the second one is used in what is probably the most well-known cryptographic algorithm in the world - AES [15]. In doing so, we experiment with three different approaches when generating S-boxes: random search, heuristics and affine transformation.

After presenting the newly generated S-boxes for both sizes, we also give SCA experiments, but only for 4×4 size. This is due to the two reasons: the first one is that our new S-box has all the same properties as the S-boxes currently used except it is superior in modified transparency order property. The second reason is that our S-box is possible to implement only as a lookup table which does not represent a difficulty for that size. When considering 8×8 size, both of those arguments do not hold.

1.1 Related Work

Leander and Poschmann classify all optimal 4×4 S-boxes [4]. Some examples of algorithms using optimal S-boxes are PRESENT [13], PRINCE [14] and Noekeon [16].

Regarding modified transparency order property, except for the paper that presented the property [17], there are currently no other works. However, when discussing the original transparency order property there are many (sometimes contradicting) results. After Prouff in 2005 defined transparency order [7], for a couple of years this property did not attract a lot of attention. However, from 2012 there have been several works exploring that property. Mazumdar et al. construct rotation symmetric S-boxes with high nonlinearity and DPA resistance [18]. The same authors use constrained random search to find S-boxes with low transparency order and high nonlinearity [19]. Picek et al. use heuristics to evolve S-boxes that have improved values of transparency order property

for 8×8 size [20] and 4×4 size [21]. The same authors investigate one more measure, namely, confusion coefficient that characterizes the resilience of S-boxes against DPA attacks [22]. Evci and Kavut show the minimal affine transformation needed to change transparency order property [23]. Nguyen et al. investigate the influence of transparency order property on Serpent-type S-boxes [24].

1.2 Our Contributions

There are two main contributions in this paper. Our first contribution is that, to our best knowledge, we are the first to generate S-boxes with improved values of modified transparency order property. In order to do that we use two techniques; heuristics and affine transformation. For the 4×4 size, we find the best possible value of modified transparency order as well as lower and upper bounds for all 16 optimal classes. The second contribution is extensive DPA analysis of several newly generated S-boxes as well as their comparison with the PRESENT S-box.

The remainder of this paper is organized as follows: Section 2 gives basic information about cryptographic properties of S-boxes. In Section 3, we present S-boxes that have improved values of modified transparency order. Furthermore, we give a comparison between several methods capable of generating S-boxes. Side-channel analysis of a number of S-boxes with improved modified transparency order values as well as PRESENT S-box is presented in Section 4. Finally, in Section 5, we conclude the paper.

2 Preliminaries

Here, we present basic notions about cryptographic properties of S-boxes that are of direct interest in this research.

2.1 Optimal S-boxes

First, it would be beneficial to offer an answer which S-boxes are actually suitable in practice. When considering 4×4 S-boxes, there exist in total $16!$ bijective S-boxes which is approximately 2^{44} options to search from. Leander and Poschmann define optimal S-boxes as those that are bijective, have linearity equal to 8 and δ -uniformity equal to 4. Since the linearity that equals 8 is the same as nonlinearity of 4, we continue using the nonlinearity property instead of the linearity. By using some shortcuts they found that all optimal S-boxes belong to 16 classes, i.e. all optimal S-boxes are affine equivalent to one of those 16 classes [4].

Therefore, for the 4×4 S-box size, we concentrate only on optimal S-boxes as those of practical interest. Indeed, as far as the authors know, all ciphers that use 4×4 S-boxes actually use optimal S-boxes [13, 14, 16, 25].

For the 8×8 size, there exists no such classification, but in general it is believed that nonlinearity of 112 is the maximum possible and therefore the best S-boxes should reach that nonlinearity [26]. There are other conditions except

the nonlinearity property, but highly nonlinear S-boxes usually also have other classical properties with good values [26,27]. In accordance to that, for the 8×8 size, we restrict our attention to the same properties as for the 4×4 size.

2.2 Cryptographic Properties of S-boxes

Here, we discuss the properties that are used to define optimal S-boxes: bijectivity, nonlinearity and δ -uniformity [4]. Besides those properties, we also formally introduce two properties that constitute the core of this research: transparency order and modified transparency order.

The addition modulo 2 is denoted as “ $\oplus$ ”. The inner product of vectors $\bar{a}$ and $\bar{b}$ is denoted as $\bar{a} \cdot \bar{b}$ and equals $\bar{a} \cdot \bar{b} = \bigoplus_{i=1}^n a_i b_i$.

Function F , called S-box or vectorial Boolean function, of size (n, m) is defined as any mapping F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ [7].

The Hamming weight HW of a vector $\bar{a}$, where $\bar{a} \in \mathbb{F}_2^n$, is the number of non-zero positions in the vector.

An (n, m) -function is called balanced if it takes every value of $\mathbb{F}_2^m$ the same number 2^{n-m} of times [26]. Balanced (n, n) -functions are permutations on $\mathbb{F}_2^n$.

Nonlinearity NL_F of an (n, m) -function F equals the minimum nonlinearity of all non-zero linear combinations $\bar{b} \cdot F$ of its coordinate functions f_i , where $\bar{b} \neq 0$ [28]:

$$NL_F = 2^{n-1} - \frac{1}{2} \max_{\substack{\bar{a} \in \mathbb{F}_2^n \\ \bar{v} \in \mathbb{F}_2^m}} |W_F(\bar{a}, \bar{v})|. \quad (1)$$

Here, $W_F(\bar{a}, \bar{v})$ represents the Walsh-Hadamard transform of F [7]:

$$W_F(\bar{a}, \bar{v}) = \sum_{\bar{x} \in \mathbb{F}_2^n} (-1)^{\bar{v} \cdot F(\bar{x}) \oplus \bar{a} \cdot \bar{x}}. \quad (2)$$

Differential delta uniformity δ represents the largest value in the difference distribution table without counting the value 2^n in the first row and first column position [1, 26, 29].

Prouff introduced transparency order property of S-boxes which can be defined for a (n, m) -function as follows [7]:

$$T_F = \max_{\bar{\beta} \in \mathbb{F}_2^m} (|m - 2HW(\bar{\beta})| - \frac{1}{2^{2n} - 2^n} \sum_{\substack{\bar{a} \in \mathbb{F}_2^{n*} \\ \bar{v} \in \mathbb{F}_2^m \\ HW(\bar{v}) = 1}} | \sum_{\bar{v} \in \mathbb{F}_2^m} (-1)^{\bar{v} \cdot \bar{\beta}} W_{D_a F}(\bar{0}, \bar{v}) |). \quad (3)$$

Here, $W_{D_a F}$ represents Walsh-Hadamard transform of the derivative of F with respect to a vector $a \in \mathbb{F}_2^n$. For further information about the transparency order property, we refer readers to [7, 28].

Recently, researchers presented modified transparency order property in order to deal with some errors in the original definition [17]. This new, modified transparency order property equals:

$$\begin{aligned}
MT_F = \max_{\beta \in \mathbb{F}_2^m} & \left(m - \frac{1}{2^{2n} - 2^n} \sum_{\bar{a} \in \mathbb{F}_2^{n*}} \right. \\
& \left. \sum_{j=1}^m |A_{F_j}(a) + \sum_{i=1, i \neq j}^m (-1)^{\beta_i \oplus \beta_j} C_{F_i, F_j}(a)| \right),
\end{aligned} \tag{4}$$

where $A_{F_j}(a)$ represents the autocorrelation function of F and $C_{F_i, F_j}(a)$ represents the crosscorrelation function. The crosscorrelation $C_{F_i, F_j}(a)$ between functions F_i and F_j equals:

$$C_{F_i, F_j}(a) = \sum_{x \in \{0,1\}^n} (-1)^{F_i(x) \oplus F_j(x \oplus a)}. \tag{5}$$

We do not give an exhaustive explanation behind the modified transparency order, but rather we enumerate main problems with the original definition of transparency order which are corrected in the new, modified measure. In [19], it was shown that the autocorrelation spectra properties of the coordinate functions have a bearing on the resistivity of the S-box towards power analysis attacks. Further, the crosscorrelation term in the modified transparency order shows that the coordinate functions when selected in a pairwise fashion, also affect the resistance to the power based side-channel attacks. Therefore, along with the differential uniformity [30], several cryptographic properties of an S-box such as the autocorrelation spectra and the crosscorrelation spectra properties also determine the side-channel resistivity of an S-box.

In the transparency order property, there is a maximization over all values of β which is shown to be redundant. Next, the crosscorrelation terms between coordinate functions is assumed to be 0 in the original definition which is not the case in general. Finally, when considering lower bound in the original transparency order, it is calculated for bent functions, but the property itself is defined only for balanced functions [17]. In the original definition of the transparency order, the coordinate functions of an S-box are assumed to be balanced, which though correct for popular S-boxes in block ciphers, is not correct on the entire space of S-box functions. This makes the definition of original transparency order incorrect for S-boxes with unbalanced coordinate functions like bent functions. For instance, it was shown in Chakraborty et al. that for an S-box with pairwise complement coordinate functions which are bent, DPA is not possible [17]. But from the definition, transparency order is maximum for such S-boxes, which indicates high vulnerability towards the DPA attacks. This contradiction renders the original definition of transparency order incorrect.

2.3 Affine Equivalence

For two (n, n) -functions S_1 and S_2 to be affine equivalent, the following equation needs to hold:

$$S_2(x) = B(S_1(A(x) \oplus a)) \oplus b, \tag{6}$$

where A and B are invertible $n \times n$ matrices and a, b are constants in $\mathbb{F}_2^n$.

Picek et al. showed that affine transformation can be used to generate affine equivalent S-boxes that have different values of the transparency order and the confusion coefficient properties [21, 22].

3 Generating S-boxes

In this section, we use several techniques to generate S-boxes with improved modified transparency order. Furthermore, we conduct a comparison between those methods and give an analysis of the lower and upper bounds for the modified transparency order of 4×4 S-boxes.

3.1 Random Search

For random search, solutions are generated by creating uniformly at random a permutation list of values from 0 to $2^n - 1$. Distribution of the random S-boxes values is shown in Table 1 for the 4×4 size and Table 2 for 8×8 size.

Table 1. Distribution of random S-boxes property values, 4×4 , 5 000 evaluations.

Property	Max	Min	Mean	Std. dev.
NL_F	4	0	2.1	0.69
δ -uniformity	16	4	6.7	1.37
MT_F	2.93	1.6	2.44	0.14

Table 2. Distribution of random S-boxes property values, 8×8 , 1 000 evaluations.

Property	Max	Min	Mean	Std. dev.
NL_F	98	84	92.57	2.13
δ -uniformity	16	10	11.37	1.21
MT_F	6.9	6.83	6.86	0.01

3.2 Genetic Algorithm

In accordance with the related works, e.g. [21, 31], we experiment with heuristics to evolve S-boxes that have good modified transparency order values. For the algorithm of the choice, we use genetic algorithm (GA) since it proved to be a good choice in related works. We emphasize that the genetic algorithm does not necessarily represent the best possible approach how to solve this problem, but rather an option one has at his disposal. For a detailed explanation about genetic algorithms, we refer interested readers to [32].

To represent the problem, we use a permutation representation where an S-box is represented with decimal values between 0 and $2^n - 1$, where each of those values is one entry for the S-box lookup table. For the permutation representation, a mutation operator is selected uniformly at random between insert and inversion mutation [32]. Recombination operator is selected uniformly at random between the partially mapped crossover (PMX) [33] and order crossover OX [34]. Both of those crossover operators are among the most common ones for the permutation encoding.

Fitness Functions. When investigating 4×4 size, fitness function combines all the properties that the optimal S-box must have plus the modified transparency order. The goal is to *maximize* the following function:

$$fitness = NL_F + (n - MT_F) + (2^n - \delta). \quad (7)$$

We subtract MT_F and δ -uniformity values from the maximum obtainable values since we represent the problem as a maximization problem and those properties need to be as small as possible.

For the 8×8 case, fitness function equals the sum of nonlinearity (N_F) and modified transparency order as follows:

$$fitness = NL_F + (n - MT_F). \quad (8)$$

For this size, we do not add δ -uniformity to the equation since all our experiments show that it does not help in converging to better solutions, but just makes the evolution process longer.

Common Parameters. Parameters for the GA are the following: the sizes of (n, n) -function are 4 and 8, number of independent runs for each evolutionary experiment is 50 and the population size is 50. Tournament size in steady-state tournament selection is equal to 3. Mutation probability is set to 0.3 per individual. This mutation rate is set on a basis of tuning phase where it showed good results. The evolution process lasts until there is 50 generations without improvement of the best solution. Common parameters are additionally given in Table 3.

3.3 Evolved S-boxes

For the 4×4 size, the best value of modified transparency order we found with the genetic algorithm is 1.9 for an optimal S-box. The transparency order and the modified transparency order values for our evolved S-box as well as for the PRESENT S-box and random S-box are presented in Table 4.

Next, in Table 5, we display a solution that have the best modified transparency order (1.9) property that we found with the genetic algorithm and that belongs to the one of the optimal classes.

As it can be seen, for the 4×4 size, it is possible to obtain S-box that has significantly lower value of modified transparency order while remaining in one

Table 3. Common parameters for GA.

Parameter	Parameter value
Tournament size k	3
Population size	50
Number of experiments	50
Mutation probability	0.3 per individual
Stopping criterion	50 generations without improvement

Table 4. Properties of evolved S-boxes, modified transparency order, 4×4 .

S-box	MT_F	T_F
PRESENT	2.467	3.53
Random S-box	2.44	3.47
Evolved S-box	1.9	3.267

Table 5. S-box evolved with the genetic algorithm.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S(x)	2	0	C	6	A	E	F	7	3	1	8	4	9	D	B	5

of the optimal classes. Next, we display results for the 8×8 size in Table 6. As it can be seen, in this case properties like the nonlinearity, δ -uniformity, GAC (Δ_F and σ_F) [35] significantly deteriorate for the evolved S-boxes. In Figures 1 and 2, we display results for random, AES and evolved S-boxes for sizes 4×4 and 8×8 , respectively.

3.4 Affine Transformations

It has been shown that the transparency order property is not affine invariant under certain affine transformations [21]. Therefore, we investigate whether the same applies when considering modified transparency order property. We apply four affine transformations as given in [21], where we see that the transformations 3 and 4 change the modified transparency order values (as is the case for the transparency order property [21]). Those affine transformations are based on Eq. (6).

By following the reasoning from [23], we observe that we can apply the same transformation as in that work in order to conduct an exhaustive search. That affine transformation has the following form:

$$S_2(x) = B(S_1(x)). \quad (9)$$

Note that the affine transformation in Eq. (9) is the special form of transformations 3 and 4 from [21] where constants c and d equal 0 and matrix B is the identity matrix.

Table 6. Properties of evolved S-boxes, modified transparency order, 8×8 .

S-box	NL_F	MT_F	T_F	δ	Δ_F	σ_F
AES S-box	112	6.916	7.86	4	32	133120
Random S-box	92	6.869	9.173	12	96	272128
Evolved S-box 1	100	6.815	7.761	10	104	258304
Evolved S-box 2	98	6.67	7.7	14	96	272896

Fig. 1. Nonlinearity versus modified transparency order, 4×4 .

Fig. 2. Nonlinearity versus modified transparency order, 8×8 .

Results of exhaustive search for all 16 optimal classes' lower and upper bounds are given in Table 7. Additionally, we offer results for class representatives where G_1 to G_{15} are the usual acronyms for the 16 optimal S-box classes.

Table 7. Modified transparency values, 4×4 size.

S-box	MT_F		
	Min	Max	Class representative
G_0	2.067	3	2.23
G_1	1.9	2.8	2.53
G_2	2.03	2.867	2.56
G_3	2.4	2.8	2.46
G_4	2.3	2.83	2.56
G_5	2.33	2.93	2.53
G_6	2.23	2.73	2.46
G_7	2.26	2.7	2.53
G_8	2.03	2.867	2.3
G_9	2.167	2.8	2.5
G_{10}	2.167	2.767	2.36
G_{11}	2.23	2.667	2.46
G_{12}	2.33	2.83	2.5
G_{13}	2.26	2.9	2.66
G_{14}	2.2	2.93	2.6
G_{15}	2.13	2.9	2.5

We see there is only one class that reaches the minimal value of 1.9 and there are 10 different maximal values over all classes. In Figure 3, we give a frequency distribution of all values under the affine transformation from Eq. (9) for the optimal class G_1 .

Note that the best value from the exhaustive search is the same as from the genetic algorithm. This shows that such heuristics should present a viable choice when generating S-boxes of comparable sizes. For larger sizes we believe heuristics like genetic algorithms are not appropriate. This stems from two important facts. The first one is that the generated S-boxes have significantly worse values for properties like the nonlinearity and δ -uniformity. The second reason is that the equation for calculating the modified transparency order is much more complex and computationally demanding than in the case of e.g. original transparency order property. This results in relatively slow evaluation of the modified transparency order property, a fact not so important when it is necessary to

Fig. 3. Frequency distribution of MT_F values for the class G_1 .

run the equation only a several times. However, for heuristics like genetic algorithm where the number of evaluations can be rather large, this means the whole process will be long.

When considering 8×8 size, it is not possible to conduct an exhaustive search since the search space is still to large. Therefore, we run experiment with the affine transformation as for the 4×4 size, but for 1 000 randomly generated B matrices. The best value we found equals 6.89 (while AES S-box has 6.916).

4 Success Rate Evaluation of DPA Attacks on the Synthesized S-boxes

In this section, we evaluate the generated 4×4 S-boxes when these S-boxes are subjected to key-recovery attacks like differential power analysis (DPA) in the form of statistical analysis of the physically observables like power traces to efficiently discriminate the secret key. In this set of experiments, we consider Pearson's coefficient as the statistical analysis parameter.

In this experiment, we consider the standalone module of an S-box to which the input is the XOR of the secret key and the input message. We employ the security metric called success rate to measure how easily the physical observable can be turned into a successful attack [36]. The efficiency of a side-channel attack to reach a certain success rate (e.g. 80%) is the minimum average number of queries such that the success rate of this attack attains the value (80%). Here, we measure this efficiency of the DPA attacks in terms of number of queries required to extract the secret key.

We inspect the Gaussian noise distribution $\mathbf{N}$ with zero mean and standard deviation σ added to the Hamming weight of the S-box output $S(x \oplus k)$ as the physically observable power trace. From the literature, this is the standard power model for hardware implementation and as for the software implementation, this power model in the microprocessor is applied on each instruction execution [3].

In order to evaluate the success rate, we observe the number of successful attempts to extract the secret key out of several random attempts to attack on an average. The success rate of the correlation analysis DPA attacks with noise with standard deviation values from 0.1 to 2.0 on the synthesized S-boxes is shown in Fig. 4. We also perform the same experiment on the PRESENT 4×4 S-box whose results are shown in Fig. 5. In comparison of success rate results in both the figures, we find that in the presence of noise with high standard deviation, the success rate of DPA attacks of the synthesized S-boxes is less than that of the PRESENT S-boxes.

From Table 8, for Gaussian noise with standard deviation as high as 2.0, the maximum success rate attained in our class of synthesized S-boxes is less than half of that of PRESENT S-box. In the case the standard deviation of the Gaussian noise is small, the number of queries required to attain a success rate of 80% in case of our synthesized S-boxes is lesser compared to the PRESENT S-box. Furthermore, in the same table we give data about the transparency order and confusion coefficient values for all S-boxes. We can observe that the properties are not in line, e.g. different properties point that different S-boxes have the best DPA resistance. Further, the success rate for small number of queries is very small in both PRESENT S-box as well as our class of synthesize S-boxes. Also, contrary to the fact that the success rate of correlation DPA should increase with increasing number of queries, the dip in success rates (especially for PRESENT S-box) is significant for some regions of increasing queries. Similar results were observed in existing literature for classification rates of S-boxes with increasing number of queries [37].

Table 8. Comparison of modified transparency order parameter with success rates of the DPA attacks

S-box	T_F	MT_F	Conf. coeff.	# queries to reach 100% success rate (SD=0.1)	Max success rate (SD=2.0)
PRESENT	3.533	2.467	1.709	8	65%
S-box 1	3.267	1.9	1.145	8	28%
S-box 2	3.4	2.167	1.615	10	32%
S-box 3	3.333	2.2	1.615	8	35%
S-box 4	3.4	2.233	1.145	7	34%
S-box 5	3.467	2.267	1.145	6	32%
S-box 6	3.467	2.3	0.956	11	34%

(a) Success rate plots for the correlation analysis DPA on simulated power traces of S-box 1.

(b) Success rate plots for the correlation analysis DPA on simulated power traces of S-box 2.

(c) Success rate plots for the correlation analysis DPA on simulated power traces of S-box 3.

(d) Success rate plots for the correlation analysis DPA on simulated power traces of S-box 4.

Fig. 4. Success rate plots for the correlation analysis DPA on simulated power traces of the generated S-boxes.

(e) Success rate plots for the correlation analysis DPA on simulated power traces of S-box 5.

(f) Success rate plots for the correlation analysis DPA on simulated power traces of S-box 6.

Fig. 4. (Continued)

Fig. 5. Success rate plots for the correlation analysis DPA on simulated power traces of PRESENT S-box.

Although smaller modified transparency order should result in an S-box with better DPA resistivity, our experiments show that in the case of small differences in modified transparency, such behavior is hard to obtain. This behavior is similar to that what can be observed when examining original transparency order measure. However, there are at least two advantages of using the modified transparency order. The first one is the fact the researcher would use the correct formula (although, sometimes practical results do not show significant differences between properties). The second advantage is that the correlation between the modified transparency order values and max. success rates is more easily noticeable, although not linear. The answer whether the modified transparency order property is a sufficient countermeasure against DPA attacks highly depends on the level of noise in the settings. However, we believe it is not enough (similar to other DPA related S-box properties), but instead should be used in combination with some other countermeasures like masking.

5 Conclusion

In this work, we consider the influence of the modified transparency order property to the DPA resistance of S-boxes. We generate S-boxes that have improved values of the modified transparency order where for the 4×4 size, we remain in the optimal classes. When considering 8×8 size, the improvement in the modified transparency comes at the cost of the deterioration of other properties like the nonlinearity or δ -uniformity. Furthermore, we show the minimal necessary affine transformation needed to change the modified transparency order value. Based on that transformation, we show that the value obtained by our genetic algorithm is indeed the optimal one. In doing so, we also show that only one of 16 optimal classes for the 4×4 size can reach the best possible value for modified transparency. We use the same affine transformation to find the upper and lower bound for modified transparency order for all 16 optimal classes. Finally, we conduct practical SCA experiments with our new S-boxes as well as with the PRESENT S-box. From the results, we observe that the number of necessary traces for the successful attack is significantly lower for our S-boxes than for the PRESENT S-box in the presence of noise. Although our results indicate that the modified transparency order is more reliable measure than the original transparency order, we still do not deem it sufficiently strong to be considered without other countermeasures.

Acknowledgments. This work was supported in part by the Technology Foundation STW (project 12624 - SIDES), The Netherlands Organization for Scientific Research NWO (project ProFIL 628.001.007) and the ICT COST action IC1204 TRUDEVICE.

References

1. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. In: Menezes, A., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 2–21. Springer, Heidelberg (1991)
2. Matsui, M., Yamagishi, A.: A new method for known plaintext attack of FEAL cipher. In: Rueppel, R.A. (ed.) EUROCRYPT 1992. LNCS, vol. 658, pp. 81–91. Springer, Heidelberg (1993)
3. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security). Springer-Verlag New York, Inc (2007)
4. Leander, G., Poschmann, A.: On the Classification of 4 Bit S-Boxes. In: Carlet, C., Sunar, B. (eds.) WAIFI 2007. LNCS, vol. 4547, pp. 159–176. Springer, Heidelberg (2007)
5. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security). Springer-Verlag New York, Inc., Secaucus (2007)
6. Guilley, S., Pacalet, R.: Differential Power Analysis Model and Some Results. In: Proceedings of CARDIS, pp. 127–142. Kluwer Academic Publishers (2004)
7. Prouff, E.: DPA Attacks and S-Boxes. In: Gilbert, H., Handschuh, H. (eds.) FSE 2005. LNCS, vol. 3557, pp. 424–441. Springer, Heidelberg (2005)
8. Kocher, P., Jaffe, J., Jun, B.: Differential Power Analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
9. Fei, Y., Luo, Q., Ding, A.A.: A statistical model for dpa with novel algorithmic confusion analysis. In: Prouff, E., Schaumont, P. (eds.) CHES 2012. LNCS, vol. 7428, pp. 233–250. Springer, Heidelberg (2012)
10. Fei, Y., Ding, A.A., Lao, J., Zhang, L.: A statistics-based fundamental model for side-channel attack analysis. IACR Cryptology ePrint Archive 2014, 152 (2014)
11. Luo, Q., Fei, Y.: Algorithmic collision analysis for evaluating cryptographic systems and side-channel attacks. In: 2011 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp. 75–80 (2011)
12. Ding, A.A., Zhang, L., Fei, Y., Luo, P.: A statistical model for higher order dpa on masked devices. IACR Cryptology ePrint Archive 2014, 433 (2014)
13. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J., Seurin, Y., Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbaauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007)
14. Borghoff, J., Canteaut, A., Gneysu, T., Kavun, E., Knezevic, M., Knudsen, L., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S., Yaln, T.: PRINCE: A Low-Latency Block Cipher for Pervasive Computing Applications. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 208–225. Springer, Heidelberg (2012)
15. Daemen, J., Rijmen, V.: The Design of Rijndael. Springer-Verlag New York, Inc., Secaucus (2002)
16. Daemen, J., Peeters, M., Assche, G.V., Rijmen, V.: Nessie proposal: the block cipher Noekeon. Nessie submission (2000), <http://gro.noekeon.org/>
17. Chakraborty, K., Sarkar, S., Maitra, S., Mazumdar, B., Mukhopadhyay, D., Prouff, E.: Redefining the transparency order. In: Coding and Cryptography, International Workshop, WCC 2015, Paris, France, April 13–17 (2015)

18. Mazumdar, B., Mukhopadhyay, D., Sengupta, I.: Design and implementation of rotation symmetric S-boxes with high nonlinearity and high DPA resilience. In: 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp. 87–92 (2013)
19. Mazumdar, B., Mukhopadhyay, D., Sengupta, I.: 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)
20. Picek, S., Ege, B., Batina, L., Jakobovic, D., Chmielewski, L., Golub, M.: On Using Genetic Algorithms for Intrinsic Side-channel Resistance: The Case of AES S-box. In: *Proceedings of the First Workshop on Cryptography and Security in Computing Systems, CS2 2014*, pp. 13–18. ACM, New York (2014)
21. Picek, S., Ege, B., Papagiannopoulos, K., Batina, L., Jakobovic, D.: Optimality and beyond: The case of 4x4 s-boxes. In: 2014 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2014, Arlington, VA, USA, May 6–7, pp. 80–83 (2014)
22. Picek, S., Papagiannopoulos, K., Ege, B., Batina, L., Jakobovic, D.: Confused by Confusion: Systematic Evaluation of DPA Resistance of Various S-boxes. In: *INDOCRYPT 2014*. LNCS, vol. 8885, pp. 374–390. Springer, Heidelberg (2014)
23. Evci, M.A., Kavut, S.: DPA Resilience of Rotation-Symmetric S-boxes. In: Yoshida, M., Mouri, K. (eds.) *IWSEC 2014*. LNCS, vol. 8639, pp. 146–157. Springer, Heidelberg (2014)
24. Nguyen, C., Tran, L., Nguyen, K.: On the resistance of serpent-type 4 bit s-boxes against differential power attacks. In: 2014 IEEE Fifth International Conference on Communications and Electronics (ICCE), pp. 542–547 (July 2014)
25. Gong, Z., Nikova, S., Law, Y.: A new family of lightweight block ciphers. In: Juels, A., Paar, C. (eds.) *RFIDSec 2011*. LNCS, vol. 7055, pp. 1–18. Springer, Heidelberg (2012)
26. Crama, Y., Hammer, P.L.: *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, vol. 1. Cambridge University Press, New York (2010)
27. Braeken, A.: *Cryptographic Properties of Boolean Functions and S-Boxes*. PhD thesis, Katholieke Universiteit Leuven (2006)
28. Carlet, C.: On highly nonlinear S-boxes and their inability to thwart DPA attacks. In: Maitra, S., Veni Madhavan, C.E., Venkatesan, R. (eds.) *INDOCRYPT 2005*. LNCS, vol. 3797, pp. 49–62. Springer, Heidelberg (2005)
29. Nyberg, K.: Perfect Nonlinear S-Boxes. In: Davies, D.W. (ed.) *EUROCRYPT 1991*. LNCS, vol. 547, pp. 378–386. Springer, Heidelberg (1991)
30. Heuser, A., Rioul, O., Guilley, S.: A theoretical study of kolmogorov-smirnov distinguishers - side-channel analysis vs. differential cryptanalysis. In: *Constructive Side-Channel Analysis and Secure Design - 5th International Workshop, COSADE 2014*, Paris, France, April 13–15, pp. 9–28 (2014) (Revised Selected Papers)
31. Picek, S., Ege, B., Batina, L., Jakobovic, D., Chmielewski, L., Golub, M.: On Using Genetic Algorithms for Intrinsic Side-channel Resistance: The Case of AES S-box. In: *Proceedings of the First Workshop on Cryptography and Security in Computing Systems, CS2 2014*, pp. 13–18. ACM, New York (2014)
32. Eiben, A.E., Smith, J.E.: *Introduction to Evolutionary Computing*. Springer, Heidelberg (2003)
33. Goldberg, D.E., Lingle, R.: Alleles, loci, and the traveling salesman problem. In: *Proc. of the International Conference on Genetic Algorithms and their Applications*, Pittsburgh, PA, pp. 154–159 (1985)

34. Davis, L.: Applying adaptive algorithms to epistatic domains. In: Proceedings of the 9th International Joint Conference on Artificial Intelligence, IJCAI 1985, pp. 162–164. Morgan Kaufmann Publishers Inc., San Francisco (1985)
35. Zhang, X., Zheng, Y.: GAC-the criterion of global avalanche characteristics of cryptographic functions. *Journal of Universal Computer Science* 1(5), 316–333 (1995)
36. Standaert, F.X., Malkin, T.G., Yung, M.: A unified framework for the analysis of side-channel key recovery attacks. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 443–461. Springer, Heidelberg (2009)
37. Kim, Y., Sugawara, T., Homma, N., Aoki, T., Satoh, A.: Biasing power traces to improve correlation in power analysis attacks. In: First International Workshop on Constructive Side-Channel Analysis and Secure Design COSADE 2010, pp. 77–80 (2010)