Constrained Search for a Class of Good S-Boxes with Improved DPA Resistivity

Bodhisatwa Mazumdar, Debdeep Mukhopadhyay and Indranil Sengupta

Dept. of Computer Science and Engineering
Indian Institute of Technology Kharagpur, India.
{bodhisatwa,debdeep}@cse.iitkgp.ernet.in, isg@iitkgp.ac.in

Abstract. In FSE 2005, *transparency order* was proposed as a parameter for the robustness of S-boxes to *Differential Power Analysis* (DPA): lower *transparency order* implying more resistance. However most cryptographically strong Boolean functions have been found to have high *transparency order*. Also it is a difficult problem to search for Boolean functions which are strong cryptographically, and yet have low *transparency order*, the total search space for (n, n)-bit Boolean functions being as large as $n2^{2^n}$. In this paper we characterize *transparency order* for various classes of Boolean functions by computing the upper and lower bounds of *transparency order* for both even and odd numbers of variables. The transparency order is defined in terms of *diffusion* properties of the structures of Boolean functions namely the number of bit flips in the output of the functions corresponding to the number of bit flips at the input of the function. The calculated bounds depend on the number of vectors flipping the input of S-box for which bias of probability of S-box output bit deviates from the value of 0.5. The *transparency order* is found to be high in the class of those Boolean functions which have larger cardinality of input differences for which the probability of output bit flip is 0.5. Also we find that instead of *propagation characteristics*, *autocorrelation spectra* of the S-box function F is a more qualifying candidate in deciding the characteristics of *transparency order*. The relations developed to characterize *transparency order* aid in our constrained random generation and search of a class of balanced 8×8 S-boxes with *transparency order* upper bounded by 7.8, *nonlinearity* in range $(104, 110)$ and *absolute indicator values* of *GAC* in range $(48, 88)$.

Keywords: Transparency Order, SNR(DPA), Hamming Weight, Walsh Transform, Nonlinearity, Propagation Criteria, Global Avalanche Characteristics.

1 Introduction

In 1996, alongwith the conventional cryptanalysis like linear [20] and differential [3] cryptanalysis, another class of threats for block cipher implementations appeared in the cryptographic community called the side channel attacks like timing [16], DPA [17] and electromagnetic radiation [26] attacks. Most prominent in this class were the DPA attacks which still render newly devised cryptosystems vulnerable because of leakages from physical hardware implmentations [18]. In this respect, efficient and leakage-minimized implementation of standard block ciphers like AES is a well studied problem [6, 23]. Also in the approach called *masking* [1], implementations of AES were protected against DPA by randomizing all intermediate data occurring during the computation of the algorithm. After this, numerous masking schemes have been proposed [4,13,23]. Meanwhile new attacking techniques were improved and defeated many of these countermeasures [5, 19] which started the *cat-and-mouse game*: new side-channel attacks developed and subsequent countermeasures proposed. In this paper, instead of countermeasures, we attempt to develop characteristics of Boolean functions for block cipher primitives of S-boxes which aim at lowering *transparency order* thus increasing robustness to DPA attacks. The design of block cipher cryptosystems embedded in cyptographic devices relies on two fundamental postulates introduced by Shannon [29]: *confusion* and *diffusion.* Whereas *confusion* makes the relationship between the key and the ciphertext as complex as possible, *diffusion* involves spreading out a disturbance done at input to the ciphertext as much as possible. In a block cipher with good *diffusion*, if one bit of intermediate data is changed, then the ciphertext should change completely, in an unpredictable or pseudorandom manner. Both these characteristics are quantified by properties of Boolean functions of the cipher primitives. *Confusion* is measured by *nonlinearity* of the Boolean function i.e. the minimum *Hamming distance* of the function from all the affine functions on the same set of input variables. *Diffusion* relates to the *propagation characteristics* [7] of the Boolean functions i.e. probability of bit flip at the output of the primitive when one or more bits are flipped at the input of the primitive.

In theoretical framework of side-channel analysis like developing power (*Hamming weight*, *Hamming distance*) and other leakage models [10] and side-channel distinguishers like *mutual information analysis* (MIA) [2, 12], the attack strength of adversary has been found to depend on mathematical properties of S-boxes. *Transparency Order* introduced by Prouff [25] and *SNR(DPA)(F)* by Guilley et al. [14] are two parameters which quantify the resistance of S-box F to DPA attacks. Also Prouff showed that S-boxes with very high *nonlinearity* and those which satisfy *propagation criteria* (PC) of higher order are more susceptible to DPA attacks. Fan et al. [11] introduced a fast implementation method of computing the *transparency order* of an S-box. Claude Carlet [8] showed that some highly *nonlinear* S-boxes like inverse function of Rijndael S-box in AES and S-boxes with Gold functions and Kasami functions have very bad *transparency order.* Recent criteria such as the nearest rival distinguishing power based on MIA [31] uses information on data-dependent device leakage function L to construct a theoretical model M of power traces which have high similarity to observed power traces for correct key hypothesis. But these criteria do not quantify DPA resistance of structures of target intermediate functions such as the *coordinate functions* of the S-boxes. In [21], it was experimentally validated that S-boxes with lower *transparency order* required much higher number of power traces to perform DPA attacks which explain their higher DPA resistitiviy compared to the S-boxes with high transparency order. In this light, this paper attempts to recognize characteristics of Boolean functions of block cipher primitives which define the resistance of the cipher to DPA like side channel analysis in terms of *transparency order.* We present the lower and upper bounds of *transparency order* for different S-boxes which fall in the same class of *propagation characteristics* with respect to same set of input bit flipping vectors. This means the DPA resistance of the S-boxes is bounded by their *propagation characteristics* with respect to a certain set of input bit flipping vectors or to be more precise by the *autocorrelation spectra* of the *coordinate functions* of the S-boxes. These bounds help in deciding parameters of S-boxes which form the elements of constrained random generation and search of S-boxes having both strong classical cryptographic properties like high *nonlinearity* [24, 27] as well as good robustness to DPA attacks (i.e. low *transparency order*). This also reduces the huge search space of $n2^{2^n}$ of (n, n)-*balanced functions* for S-boxes satisying the above criteria.

The paper is organized as follows. Section 2 describes the preliminaries to this paper. In Section 3, the *transparency order* of S-box F is expressed in terms of *Hamming weight* of bitflips at the output of the S-box when some bits are flipped in the input vector. Section 4 derives the upper and lower bounds of *transparency order* in terms of cardinalities of sets A_1, A_2 and A_3 classified according to the polarity of sum of *autocorrelation* of the *coordinate functions* of the S-boxes with shift vector a. In Section 5, the derived upper and lower bounds are evaluated for some standard S-box classes. Section 6 deals with experimental results of a constrained random generation and search of S-boxes with low *transparency order* and high *nonlinearity.* To sum up, Section 7 draws the contribution of the paper.

2 Preliminaries

2.1 Notation

In this paper, we study an S-box as an (n, n)-function F, mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. For every vector $x \in \mathbb{F}_2^n, n \in \mathbb{N}$, $HW(x)$ represents the *Hamming weight* of x. To every (n, n)-function F we represent it as an n-tuple $(f_1, \ldots, f_n)$ of Boolean functions on $\mathbb{F}_2^n$ called the *coordinate functions* of F, such that $F(x) = (f_1(x), \ldots, f_n(x))$ for every $x \in \mathbb{F}_2^n$.

2.2 Transparency Order

In [25], Prouff proposed a new metric to quantify the resistance of S-boxes to DPA attacks called *transparency order* of an S-box $F = (f_1, \ldots, f_n)$ on $\mathbb{F}_2^n$ as:

$$\tau_F = max_{\beta \in \mathbb{F}_2^n} \Bigg(\mid n - 2HW(\beta) \mid - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \mid \sum_{\substack{v \in \mathbb{F}_2^n \\ HW(v)=1}} (-1)^{v \cdot \beta} W_{D_a F}(0, v) | \Bigg) \tag{1}$$

where $W_{D_a F}(u, v)$ is the Fourier Transform of the sign function of the derivative of F with respect to vector $a \in \mathbb{F}_2^n$, $D_a F : x \mapsto F(x) \oplus F(x \oplus a)$.

$$W_{D_a F}(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot \{F(x) \oplus F(x \oplus a)\} \oplus u \cdot x} \tag{2}$$

Prouff showed that the *transparency order* degrades for higher values of PC. But according to [33], PC is an indicator of local properties as literature shows that Boolean functions constructed with high PC [28] still have undesirable linear structures which renders them vulnerable to the linear and differential attacks. So this paper focusses on the variation of *transparency order* depending on the variation of parameters which determine the indicators of global avalanche characteristics (GAC).

3 Preliminary Technical Results

From previous section, substituting $u = 0$ in equation (2):

$$W_{D_a F}(0, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot \{F(x) \oplus F(x \oplus a)\}} \tag{3}$$

As for every (n, n)-function F and for every vector $v \in \mathbb{F}_2^n$:

$$v \cdot F = \frac{1}{2} - \frac{1}{2}(-1)^{v \cdot F}$$

Substituting this in equation (3),

$$\begin{aligned} W_{D_a F}(u, v) &= \sum_{x \in \mathbb{F}_2^n} [1 - 2v \cdot \{F(x) \oplus F(x \oplus a)\}] \\ \Rightarrow W_{D_a F}(u, v) &= 2^n - 2 \sum_{x \in \mathbb{F}_2^n} [v \cdot \{F(x) \oplus F(x \oplus a)\}] \end{aligned} \tag{4}$$

So *transparency order* equation (1) modifies to:

$$\tau_F = \overset{max}{\beta \in \mathbb{F}_2^n} \Big(\mid n - 2HW(\beta) \mid - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \mid \sum_{\substack{v \in \mathbb{F}_2^n \\ HW(v)=1}} \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot \{\beta \oplus F(x) \oplus F(x \oplus a)\}} \mid \Big)$$

From equation (4), we have

$$\tau_F = \overset{max}{\beta \in \mathbb{F}_2^n} \Big(\mid n - 2HW(\beta) \mid - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \mid \sum_{\substack{v \in \mathbb{F}_2^n \\ HW(v)=1}} \{2^n - 2 \sum_{x \in \mathbb{F}_2^n} v \cdot \{\beta \oplus F(x) \oplus F(x \oplus a)\}\} \mid \Big)$$

$$\Rightarrow \tau_F = \overset{max}{\beta \in \mathbb{F}_2^n} \Big(\mid n - 2HW(\beta) \mid - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} |n2^n - 2 \sum_{x \in \mathbb{F}_2^n} HW(\beta \oplus F(x) \oplus F(x \oplus a))| \Big)$$

Next, we propose a theorem where we prove that $\beta = 0$ qualifies for *transparency order* value in S-boxes with *non-bent coordinate functions* which have good GAC. For this, we consider the *transparency order* expression:

$$\tau = \mid n - 2HW(\beta) \mid - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} |n2^n - 2 \sum_{x \in \mathbb{F}_2^n} HW(\beta \oplus F(x) \oplus F(x \oplus a))| \tag{5}$$

Theorem 1 *For S-boxes with autocorrelation spectra of coordinate functions f_i satisfying, $\forall a \in \mathbb{F}_2^{n*}$, $|\sum_{i=1}^{n} \Delta_{f_i}(a)| < 2^{n+1}$, the maximum value of transparency order expression occurs for $\beta = 0, 2^n - 1$.*

Proof. In equation (5) we consider the *transparency order* expression as difference of two terms:

$$\tau = t_1 - t_2$$

where

$$t_1 = \mid n - 2HW(\beta) \mid$$
$$t_2 = \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} |n2^n - 2 \sum_{x \in \mathbb{F}_2^n} HW(\beta \oplus F(x) \oplus F(x \oplus a))|$$

For all the coordinate functions (f_1, f_2, ..., f_n) where $f_i : \{0,1\}^n \rightarrow \{0,1\}$ of the S-box F : $\{0,1\}^n \rightarrow \{0,1\}^n$, if $\forall a \in \mathbb{F}_2^{n*}$, $\sum_{i=1}^{n} |\Delta_{f_i}(a)| < 2^{n+1}$, then

$$|n2^{n-1} - \sum_{i=1}^{n} (2^{n-1} - \frac{1}{2} \Delta_{f_i}(a))| < 2^n \tag{6}$$

From [33], the Hamming weight of truth table of $f_i(x) \oplus f_i(x \oplus a)$ is

$$\sum_{x \in \mathbb{F}_2^n} HW(f_i(x) \oplus f_i(x \oplus a)) = 2^{n-1} - \frac{1}{2} \Delta_{f_i}(a) \tag{7}$$

From (6) and (7) we get, $\forall a \in \mathbb{F}_2^{n*}$,

$$|n2^{n-1} - \sum_{i=1}^{n} \sum_{x \in \mathbb{F}_2^n} HW(f_i(x) \oplus f_i(x \oplus a))| < 2^n$$

$$\Rightarrow |n2^{n-1} - \sum_{x \in \mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a))| < 2^n$$

Summing over all $a \in \mathbb{F}_2^{n*}$,

$$\begin{aligned}
\sum_{a\in\mathbb{F}_2^{n*}} |n2^{n-1} - \sum_{x\in\mathbb{F}_2^n} HW(F(x)\oplus F(x\oplus a))| <& \quad 2^n(2^n-1) \\
\Rightarrow \frac{1}{2^{2n}-2^n} \sum_{a\in\mathbb{F}_2^{n*}} |n2^n - 2\sum_{x\in\mathbb{F}_2^n} HW(F(x)\oplus F(x\oplus a))| <& \quad 2 \\
\Rightarrow n - \frac{1}{2^{2n}-2^n} \sum_{a\in\mathbb{F}_2^{n*}} |n2^n - 2\sum_{x\in\mathbb{F}_2^n} HW(F(x)\oplus F(x\oplus a))| >& \quad n-2
\end{aligned}$$

This corresponds to the *transparency order* expression in equation (5) for $\beta = 0$. So for $\beta = 0$,

$$\tau > (n-2) \tag{8}$$

Now as for $\beta = 0,\ 2^n - 1$, the corresponding Hamming weight values $HW(\beta) = 0$, n, the first term in the *transparency order* expression,

$$t_1 = |n - 2HW(\beta)| = n \tag{9}$$

Now,

$$\begin{aligned}
\sum_{x\in\mathbb{F}_2^n} HW(F(x)\oplus F(x\oplus a)) =& \quad n2^n - \sum_{x\in\mathbb{F}_2^n} HW(\overline{F(x)\oplus F(x\oplus a)}) \\
\Rightarrow n2^n - 2\sum_{x\in\mathbb{F}_2^n} HW(F(x)\oplus F(x\oplus a)) =& \quad -(n2^n - 2\sum_{x\in\mathbb{F}_2^n} HW(\overline{F(x)\oplus F(x\oplus a)}))
\end{aligned}$$

$$\Rightarrow |n2^n - 2\sum_{x\in\mathbb{F}_2^n} HW(F(x)\oplus F(x\oplus a))| = \quad |n2^n - 2\sum_{x\in\mathbb{F}_2^n} HW(\overline{F(x)\oplus F(x\oplus a)})| \tag{10}$$

Now for $\beta = 0$, the second term of the *transparency order* expression,

$$t_2 = \frac{1}{2^{2n}-2^n} \sum_{a\in\mathbb{F}_2^{n*}} |n2^n - 2\sum_{x\in\mathbb{F}_2^n} HW(F(x)\oplus F(x\oplus a))| \tag{11}$$

while for $\beta = 2^n - 1$,

$$t_2 = \frac{1}{2^{2n}-2^n} \sum_{a\in\mathbb{F}_2^{n*}} |n2^n - 2\sum_{x\in\mathbb{F}_2^n} HW(\overline{F(x)\oplus F(x\oplus a)})| \tag{12}$$

From equation (10), equation (11) and equation (12), the second term of the *transparency order* expression, t_2 evaluates to the same value for $\beta = 0,\ 2^n - 1$.

Hence for both the values of β ($\beta = 0, 2^n - 1$), the first term (9) and the second term (11), (12) in the *transparency order* expression yields the same *transparency order* value.

$$\begin{aligned}
\Rightarrow \tau &= n - \frac{1}{2^{2n}-2^n}\Big(\sum_{a\in\mathbb{F}_2^{n*}} |n2^n - 2\sum_{x\in\mathbb{F}_2^n} HW(F(x)\oplus F(x\oplus a))|\Big) \\
&= n - \frac{1}{2^{2n}-2^n}\Big(\sum_{a\in\mathbb{F}_2^{n*}} |n2^n - 2\sum_{x\in\mathbb{F}_2^n} HW(\overline{F(x)\oplus F(x\oplus a)})|\Big)
\end{aligned} \tag{13}$$

So from equation (8), for $\beta = 0, 2^n - 1$, the *transparency order* expression,

$$\tau > (n-2) \tag{14}$$

Now for all other values of β ($\beta \neq 0, 2^n - 1$), as $1 \leq HW(\beta) \leq n-1$, the first term of the *transparency order* expression, t_1 satisfies

$$t_1 \leq n-2 \tag{15}$$

Also the second term of the *transparency order* expression t_2, being a sum of non-negative terms has always a non-negative value. In other words,

$$t_2 = \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} |n2^n - 2 \sum_{x \in \mathbb{F}_2^n} HW(\beta \oplus F(x) \oplus F(x \oplus a))|$$
$$\Rightarrow t_2 \geq 0$$

Now as the *transparency order* expression $\tau = t_1 - t_2$, so

$$\tau \leq t_1 \tag{16}$$

From equation (15) and equation (16), for these non-zero values of β ($\beta \neq 0, 2^n - 1$), the *transparency order* expression,

$$\tau \leq (n-2) \tag{17}$$

So from (14) and (17), $\beta = 0, 2^n - 1$ qualifies for the maximum value for the *transparency order* expression if $\sum_{i=1}^{n} |\Delta_{f_i}(a)| < 2^{n+1}$.

From here onwards, we will consider the case of $\beta = 0$ for *transparency order* of S-box F.

4 Upper and Lower Bounds of Transparency Order

From equation (13), *transparency order* of S-box $F(x)$ is expressed as:

$$\tau_F = n - \frac{1}{2^{2n} - 2^n} \left(\sum_{a \in \mathbb{F}_2^{n*}} |n2^n - 2 \sum_{x \in \mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a))| \right)$$

The set $A = \{a | a \in \mathbb{F}_2^{n*}\}$ can be represented as $A = A_1 \cup A_2 \cup A_3$ such that:

$$A_1 = \{a | a \in \mathbb{F}_2^{n*} \wedge \sum_{x \in \mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a)) < n2^{n-1}\}$$
$$A_2 = \{a | a \in \mathbb{F}_2^{n*} \wedge \sum_{x \in \mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a)) > n2^{n-1}\}$$
$$A_3 = \{a | a \in \mathbb{F}_2^{n*} \wedge \sum_{x \in \mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a)) = n2^{n-1}\}$$

The sets A_1, A_2, A_3 can also expressed in terms of *autocorrelation* of coordinate function $f_i(x)$ with shift of vector a:

$$\mathit{\Delta}_{f_i}(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f_i(x) \oplus f_i(x \oplus a)}$$

$$A_1 = \{a | a \in \mathbb{F}_2^{n*} \wedge \sum_{i=1}^{n} \mathit{\Delta}_{f_i}(a) > 0\}$$

$$A_2 = \{a | a \in \mathbb{F}_2^{n*} \wedge \sum_{i=1}^{n} \mathit{\Delta}_{f_i}(a) < 0\}$$

$$A_3 = \{a | a \in \mathbb{F}_2^{n*} \wedge \sum_{i=1}^{n} \mathit{\Delta}_{f_i}(a) = 0\}$$

Among these sets, A_3 corresponds to the set of values of vector a with respect to which S-box F satisfies PC. In other words, this set comprises of those vectors a such that probability of bit flip at output of $F(x)$ is 0.5 when exactly $HW(a)$ number of input bits are flipped at the input. In set A_1, the values of vector a correspond to the truth table of $F(x) \oplus F(x \oplus a)$ where number of zeros is greater than number of ones. In other words, A_1 represents the set of those values of vector a for which probability of bit flipping at the output of S-box is less than 0.5 when $HW(a)$ number of input bits of the S-box are flipped (i.e. $\sum_{i=1}^{n} \mathit{\Delta}_{f_i}(a) > 0$). Similarly, A_2 corresponds to the set of values of vector a for which the probability of bit flipping at the output of S-box is greater than 0.5 when $HW(a)$ number of input bits of the S-box are flipped (i.e. $\sum_{i=1}^{n} \mathit{\Delta}_{f_i}(a) < 0$).

$$\Rightarrow \tau_F = n - \frac{1}{2^{2n} - 2^n} \Bigg(\sum_{a \in A_1} \Big\{ n2^n - 2 \sum_{x \in \mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a)) \Big\} \\ - \Big\{ \sum_{a \in A_2} \Big\{ n2^n - 2 \sum_{x \in \mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a)) \Big\} \Big\} \Bigg)$$

$$\Rightarrow \tau_F = n - \frac{1}{2^{2n} - 2^n} \Bigg(n2^n (\mid A_1 \mid - \mid A_2 \mid) - 2 \sum_{a \in A_1} \sum_{x \in \mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a)) \\ + 2 \sum_{a \in A_2} \sum_{x \in \mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a)) \Bigg) \tag{18}$$

Upper Bound of Transparency Order of *S*-box: For upper bound of *transparency order* of $F(x)$, lower bound of the expression $\sum_{a \in A_2} \sum_{x \in \mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a))$ and upper bound of the expression $\sum_{a \in A_1} \sum_{x \in \mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a))$ in equation (18) is calculated. In case of *balanced* $F(x) \oplus F(x \oplus a)$ (i.e. $a \in A_3$), the truth table has *Hamming weight* $n2^{n-1}$. But when $a \in A_2$, the lower bound of *Hamming weight* of truth table of $F(x) \oplus F(x \oplus a)$ is just one more than $n2^{n-1}$ ($\forall a \in A_2$, number of ones is greater than number of zeros in truth table of $F(x) \oplus F(x \oplus a)$). But in truth table of $F(x) \oplus F(x \oplus a)$ *Hamming weight* can only be even as each entry in truth table occurs exactly twice. So the lower bound of the *Hamming weight* will be two more than $n2^{n-1}$. So $\forall a \in A_2$,

$$\sum_{x \in \mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a)) \geq n2^{n-1} + 2 \tag{19}$$

Similarly $\forall a \in A_1$, the upper bound of $HW(F(x) \oplus F(x \oplus a))$ occurs when the *Hamming weight* of truth table of $F(x) \oplus F(x \oplus a)$ is just two less than $n2^{n-1}$. So $\forall a \in A_1$,

$$\sum_{x \in \mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a)) \leq n2^{n-1} - 2 \tag{20}$$

Substituting equation (19) and equation (20) in equation (18), *transparency order* of $F(x)$ satisfies:

$$\tau_F \leq n - \frac{4}{2^{2n} - 2^n}\Big\{ \mid A_1 \mid + \mid A_2 \mid \Big\} \Rightarrow \tau_F \leq n - \frac{4}{2^{2n} - 2^n}\Big\{ 2^n - 1 - \mid A_3 \mid \Big\}$$

This upper bound is interesting as it is tighter than the known upper bound of $\tau \leq n$ mentioned by Prouff; the equality holding for bent functions. The upper bound of *transparency order* reduces when for lesser number of vectors a, the truth table of $F(x) \oplus F(x \oplus a)$ is *balanced* (i.e. when $|A_3|$ is small). In other words, Boolean functions satisfying PC of higher order (i.e. high $|A_3|$) has higher *transparency order* which is in agreement with observation made by [25]. But this is not the only case in which *transparency order* is high. Even with $F(x)$ not satisfying PC of higher order, if the derivative $F(x) \oplus F(x \oplus a)$ is *balanced* for large number of vectors a, then also *transparency order* is high. For PC of order 1, $F(x) \oplus F(x \oplus a)$ is *balanced* for a where $HW(a) = 1$. There are $\binom{n}{1}$ possible values of a which satisfy this condition. Similarly for PC of order k, $F(x) \oplus F(x \oplus a)$ is *balanced* for $1 \leq HW(a) \leq k$ which comprise of $\binom{n}{1} + \ldots + \binom{n}{k}$ values of a. If $F(x) \oplus F(x \oplus a)$ is not *balanced* for above set of values of a, but for a different set of values of a with the same cardinality, the condition of PC of order k is not satisfied but still the *transparency order* is high. So instead of PC, we believe *autocorrelation* of $F(x)$ with shift of vector a is a more qualifying candidate to decide characteristics of *transparency order*. The *autocorrelation function* is also the basic parameter of indicators of global avalanche characteristics (GAC) [33].

Lower Bound of Transparency Order of S-box (even n): For lower bound of *transparency order* of S-box $F(x)$, the lower bound of the expression
$\sum_{a \in A_1} \sum_{x \in \mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a))$
and the upper bound of
$\sum_{a \in A_2} \sum_{x \in \mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a))$
in equation (18) is calculated. As in case of even n ,$\forall a \in A_2$,

$$\sum_{x \in \mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a)) \leq 2 \sum_{i=0}^{\frac{n}{2}-1} (n-i)\binom{n}{i} + \frac{n}{2}\binom{n}{\frac{n}{2}}$$

In this, there are $2\binom{n}{i}$ combinations of x for each of the *Hamming weight* values from n to $(\frac{n}{2}+1)$ and for *Hamming weight* value of $\frac{n}{2}$, there are $\binom{n}{\frac{n}{2}}$ combinations of x which yield maximum value of $HW(F(x) \oplus F(x \oplus a))$.

For even n, $\forall a \in A_1$,

$$\sum_{x \in \mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a)) \geq 2 \sum_{i=1}^{\frac{n}{2}-1} i\binom{n}{i} + \frac{n}{2}\Big\{\binom{n}{\frac{n}{2}} + 2\Big\}$$

In this, there are $2\binom{n}{i}$ combinations of x for each of the *Hamming weight* values from 1 to $(\frac{n}{2}-1)$ and for *Hamming weight* value of $\frac{n}{2}$, there are $\binom{n}{\frac{n}{2}}+2$ combinations of x which yield minimum value of $HW(F(x) \oplus F(x \oplus a))$.

So the *transparency order* of $F(x)$ satisfies:

$$\tau_F \geq n - \frac{1}{2^{2n}-2^n}\Bigg\{n2^n(\mid A_1 \mid - \mid A_2 \mid) + 2\Bigg(\mid A_2 \mid \Bigg(2\sum_{i=0}^{\frac{n}{2}-1}(n-i)\binom{n}{i} + \frac{n}{2}\binom{n}{\frac{n}{2}}\Bigg) - \mid A_1 \mid \Bigg(2\sum_{i=1}^{\frac{n}{2}-1} i\binom{n}{i} + \frac{n}{2}\Bigg(\binom{n}{\frac{n}{2}}+2\Bigg)\Bigg)\Bigg)\Bigg\}$$

So the lower bound of *transparency order* of S-box $F(x)$ depends on cardinalities of sets A_1 and A_2. In other words, the minimum value of *transparency order* for a particular n depends on the number of vectors a for which bias of probability of bit flipping at the output of S-box deviates from 0.5 when $HW(a)$ number of input bits are flipped at the input.

Lower Bound of Transparency Order of S-box (odd n): In case of odd n, the bounds of *Hamming weight* values in previous section differ.

For odd n, $\forall a \in A_2$,

$$\sum_{x\in\mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a)) \leq 2\sum_{i=0}^{\lfloor n/2 \rfloor}(n-i)\binom{n}{i}$$

In this case, for each of the *Hamming weight* values from i = 0 to $n - \lfloor n/2 \rfloor$, there are $2\binom{n}{i}$ combinations of x which $\forall a \in A$ yields maximum value of $\sum_{x\in\mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a)), a \in A_2$.

Also $\forall a \in A_1$,

$$\sum_{x\in\mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a)) \geq 2\Bigg(\sum_{i=1}^{\lfloor n/2 \rfloor} i\binom{n}{i} + \left\lceil \frac{n}{2} \right\rceil\Bigg)$$

In this case, for each of the *Hamming weight* values from i = 1 to $\lfloor n/2 \rfloor$, there are $2\binom{n}{i}$ combinations of x and for *Hamming weight* $\lceil n/2 \rceil$ there are two combinations of x which $\forall a \in A_1$ leads to minimum value of $\sum_{x\in\mathbb{F}_2^n} HW(F(x) \oplus F(x \oplus a))$.

So the *transparency order* of $F(x)$ satisfies:

$$\tau_F \geq n - \frac{1}{2^{2n}-2^n}\Bigg\{n2^n(\mid A_1 \mid - \mid A_2 \mid) + 4\Bigg(\mid A_2 \mid \sum_{i=0}^{\lfloor n/2 \rfloor}(n-i)\binom{n}{i} - \mid A_1 \mid \Bigg(\sum_{i=1}^{\lfloor n/2 \rfloor} i\binom{n}{i} + \left\lceil \frac{n}{2} \right\rceil\Bigg)\Bigg)\Bigg\}$$

5 Upper and Lower Bounds of Transparency Order on Standard S-box Classes

In this section we evaluate upper and lower bounds on some classes of 8×8 S-boxes which contain standard S-boxes like AES-128 block cipher [9] and CLEFIA block cipher [30]. This class is defined to contain those S-boxes whose probability of bit flipping at the output is the same when some bits are flipped at the input of the S-box. With respect to previous section, this means the S-boxes which have the same $|A_1|$, $|A_2|$ and $|A_3|$ fall into the same class. In Table 1, lower bounds of *transparency order* with smaller values show that some S-boxes in the class have higher resistance to DPA attacks.

Table 1. *Transparency Order* bounds on some classes of 8 × 8 S-boxes

S-box Class	$\tau_{UpperBound}$	$\tau_{LowerBound}$	τ_{Sbox}	$\lvert A_3\rvert$	$\lvert A_2\rvert$
AES-128 Rijndael	7.986	6.016	7.860	21	138
CLEFIA Sbox S0	7.985	5.909	7.745	8	134
CLEFIA Sbox S1	7.985	5.980	7.852	17	148
FOX Sbox [15]	7.985	5.992	7.788	19	135

We find that not only S-boxes satisfying PC of higher orders have high *transparency order* as found out by [25], S-boxes which have *balanced* truth table of $F(x) \oplus F(x \oplus a)$ for more number of vectors a have higher *transparency order* even if they don't satisfy higher orders of PC. This is clear from lower bound plots of *transparency order* in Fig. 4 to Fig. 11 (in Appendix Section) for 8×8 S-boxes where we find that the lower bound of *transparency order* increases with increasing $|A_3|$ corresponding to same $|A_2|$. In Fig. 11, the lower and upper bound of *transparency order* has the same value (i.e. 8). This class of S-boxes correspond to bent functions, where $F(x) \oplus F(x \oplus a)$ is *balanced* for all possible values of vector a (i.e.$|A_3| = 255, |A_2| = 0, |A_1| = 0$) and so have the maximum possible value of *transparency order* [25]. Also for a class of S-boxes having *balanced* truth table of $F(x) \oplus F(x \oplus a)$ for same number of vector a (i.e. same $|A_3|$, $|A_3| \neq 255$), the lower bound of *transparency order* is found to decrease when the S-box has positive bias of probability of out bit flip for more number of vectors a i.e. when the cardinality of set A_2 increases. This decrease in lower bound for increasing $|A_2|$ can be seen in the lower bound plots of *transparency order* in Fig. 4 to Fig. 10 (in Appendix Section) for S-boxes with $n = 8$ number of input variables.

6 Experimental Results

In the previous section, it was discussed that the lower bound plots of *transparency order* have a negative slope with respect to $|A_2|$. So for higher values of $|A_2|$ corresponding to a fixed value of $|A_3|$, the lower bounds have smaller values. This means that higher values of $|A_2|$ when being constrained for search of S-boxes reduces the search space of (n, n)-Boolean functions from $n2^{2^n}$. In experiments, we adopted a constrained random S-box generation phase followed by an S-box searching phase to look for a class of 8 × 8 S-boxes which has good resistive properties both towards classical cryptanalysis as well as DPA attacks. The entire experiment of S-box generation and search was repeated 100 times to determine the cryptographic properties of the class of selected S-boxes. Each simulation run of generating a pool of 2^{20} S-boxes and further searching takes around 5hr 37mins on 2.3GHz Intel Core i5-2410M processor with 4GB RAM. The algorithm was implemented in C programming language and compiled using gcc-4.4.1 on Ubuntu 10.4 operating system.

6.1 Constrained Random Generation Phase

In each experiment, firstly in the S-box generation phase, $2^{20}, 8 \times 8$ *balanced* S-boxes (constrained to high values of $|A_2|$) were generated randomly which were classified according to their $|A_3|$. We opted for constrained random generation of S-boxes because on an average, randomly selected *balanced* Boolean functions has strong cryptographic properties like high *nonlinearity* [22] and for a single output *balanced* Boolean function the expected value of different forms of information leakage exponentially decreases with n i.e. number of input variables [32]. The number of generated S-boxes has a normal distribution with respect to $|A_3|$ as shown in Fig. 12 in Appendix Section. The plot shows that all values of $|A_3|$ do not occur which leads to reduced search space and this helps in selecting the range of $|A_3|$ for which S-boxes will be generated. The plot of S-boxes with minimum *transparency order* and the corresponding cardinalities $|A_2|$ for each value of $|A_3|$ in an experiment is shown in Fig. 13 in Appendix Section. In this figure, corresponding to each value of $|A_3|$, the minimum *transparency order* is obtained for high values of $|A_2|$ as was mentioned in the analysis of the lower and upper bounds of *transparency order* in the previous section.

6.2 S-Box Searching Phase

In the S-box searching phase, we implemented a mono-objective optimization algorithm on the generated S-box class for searching S-boxes which satisfy the objective function in Algorithm 1. The objective function was targetted on two parameters: *nonlinearity* of the *coordinate functions* of the S-box and the *transparency order* of the S-box. As high *nonlinearity* resists *linear cryptanalysis*, the *nonlinearities* of the *coordinate functions* of the S-box $(NL_1, NL_2, \ldots, NL_n)$ has been considered in objective function. In this the minimum of the *nonlinearities* of all the *coordinate functions* is targetted for maximization as shown in step 4 in Algorithm 1. This ensures higher *nonlinearity* for other *coordinate functions* also. In experiments, we find that maximizing the minimum of *nonlinearities* of *coordinate functions* yields S-boxes with better cryptographic properties than maximizing the sum of *nonlinearities* of the *coordinate functions* of the S-boxes in the search space of 2^{20} S-boxes. Also to thwart DPA attacks, *transparency order* of the S-box should be as low as possible, for which the polarity of *transparency order* of S-box is taken negative since the objective function gets maximized for lower *transparency order* values.

But for good GAC as the sum of squares indicator σ_{f_i} has to be as close to the minimum value i.e. 2^{2n} [33], the cardinality $|A_3|$ should be as high as possible while having low $|A_2|$. So a tradeoff of low *transparency order*, high $|A_3|$ and low $|A_2|$ is done on the class of S-boxes obtained from above searching phase. This yields another class of 8×8 S-boxes which have their GAC absolute indicator values (Δ_{f_i}) in the range (48,88) (close to 2^{n-2} for $n = 8$) as shown in Fig.2 which help in resisting differential cryptanalysis. Also the sum of the squares indicator (σ_{f_i}) for each coordinate function of the S-box is found to be within range $(2^{2n+1}$,$2^{2n+2})$ for $n = 8$.

The *nonlinearity* plot of the *coordinate functions* of the selected S-boxes in searching phase is shown in Fig. 3. As shown, for almost all experiments, we find the *nonlinearity* of the *coordinate functions* of the S-boxes to lie within the range $(2^{n-1} - 2^{\frac{n}{2}+1} + 2^{\frac{n}{2}-1}, 2^{n-1} - 2^{\frac{n}{2}} - 2)$ (i.e.$(104, 110)$ for $n = 8$). The algebraic degree of the *coordinate functions* of the S-boxes was either 6 or 7 and the robustness to *differential cryptanalysis* of the searched S-boxes was above 0.95. It may also be noted that nonlinearity, algebraic degree and robustness to differential cryptanalysis for AES Rijndael S-box are 112, 7, and 0.98 respectively. Also the *transparency order* values of the obtained S-boxes is upper bounded by 7.8 as shown in Fig. 1. For AES Rijndael S-box, *transparency order* value is 7.86 [8] which means better DPA resistance of our proposed class of S-boxes compared to AES S-box. But minimum value of *transparency order* (i.e. zero in case of linear S-boxes) does not ensure absolute resistance

Algorithm 1: Steps of Constrained Random Generation and Search of S-boxes with Low *Transparency Order*, High *Nonlinearity* and Good *GAC* characteristics

```
Input: n
Output: $F(x)$ with low transparency order (TO), high nonlinearity and minimal indicator
        values of $GAC$
Select the range of $|A_3|$ to be satisfied by generated S-boxes
for each value of $|A_3|$ do
    Randomly generate S-boxes with high values of $|A_2|$.
    Select S-box satisfying the objective function :
        $maximize[min(NL_1, NL_2, \ldots, NL_n) - TO]$
Sort the S-boxes with increasing TO.
Select the S-box $F(x)$ with optimal tradeoff between small TO, large $|A_3|$ and small $|A_2|$ for
good $GAC$.
```

of the S-box towards DPA; it means linear S-boxes are least vulnerable to DPA attacks. So for the generated S-boxes, we also computed SNR(DPA) whose lower values ensure lesser DPA discrimination power of the S-boxes [14]. The paper proposed a DPA model which reveal the correlation of one bit of predicted plaintext with the Hamming weight of the full plaintext. In the proposed class of S-boxes, we find from Fig. 1 that for most of the cases, the SNR(DPA) is lesser than that of AES Rijndael S-box i.e. 9.6. So our constrained random generation and search algorithm finds a class of S-boxes which have better resistance to DPA attacks in terms of *transparency order* and SNR(DPA) than AES Rijndael S-box while having comparable conventional cryptographic properties.

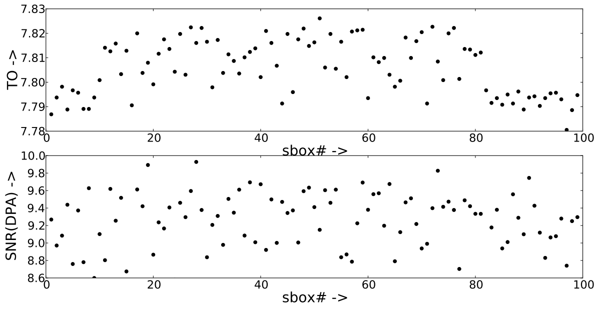

Fig. 1. *Transparency Order* and SNR(DPA) plots of 8 × 8 S-boxes selected in the searching phase

7 Conclusion

In this paper, we find that the parameter to define resistance of S-boxes to DPA attacks, *transparency order* depends on *Hamming weight* of truth table of the function $F(x) \oplus F(x \oplus a)$ where a is a vector such that *Hamming weight* of a number of input bits of S-box are flipped. The *transparency order* of S-box is also found to depend on the cardinalities of sets A_1, A_2 which correspond to vectors a such that the probability of bit flipping of the output bits of S-box is less or more than 0.5 respectively. Also, the upper and lower bounds of *transparency*

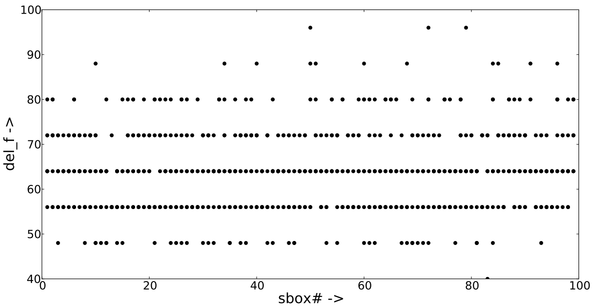

Fig. 2. *GAC* absolute indicator plots (Δ_{f_i}) of *coordinate functions* of 8×8 S-boxes selected in the searching phase

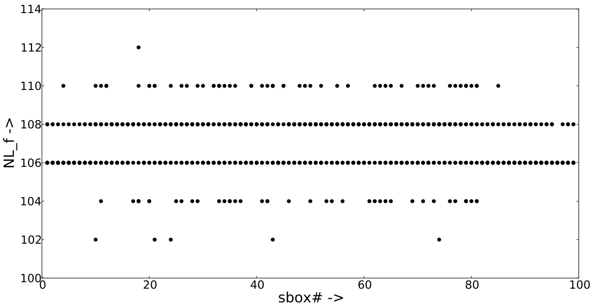

Fig. 3. Nonlinearity plots of *coordinate functions* of 8×8 S-boxes selected in the searching phase

order of *S*-boxes is calculated. We made an extension of the observation made by Prouff et al. [25] for S-boxes which have higher *transparency order*. In the analysis of lower and upper bounds of *transparency order*, we find that there is higher probability of finding an S-box with low *transparency order* when $|A_2|$ is higher. This argument is supported by the analysis of experimental results where for $|A_2|$-constrained randomly generated S-boxes with certain values of $|A_3|$, we find lesser values of *transparency order* compared to AES Rijndael S-box. Also a search algorithm is presented to find a class of S-boxes which maximizes the objective function targetted for high *nonlinearity* and low *transparency order*. The resulting class of S-boxes is then subjected to further pruning for good *diffusion* characteristics in terms of absolute indicator values (Δ_{f_i}) and sum of squares values (σ_{f_i}) of *GAC* of the coordinate function f_i of the S-box. We believe that similar approaches of constrained random generation and search of S-boxes with a suitable multiobjective optimization approach targetting high *nonlinearity* or other cryptographic properties as well as low *transparency order* or low SNR(DPA) present a future scope of finding S-boxes (and thus reducing the search space of S-boxes) with increased robustness to DPA attacks and stronger cryptographic properties.

References

1. Mehdi-Laurent Akkar and Christophe Giraud. An Implementation of DES and AES, Secure Against Some Attacks. In *CHES*, pages 309–318, 2001.
2. Lejla Batina, Benedikt Gierlichs, Emmanuel Prouff, Matthieu Rivain, François-Xavier Standaert, and Nicolas Veyrat-Charvillon. Mutual Information Analysis: A Comprehensive Study. *J. Cryptology*, 24(2):269–291, 2011.

3. Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *J. Cryptology*, 4(1):3–72, 1991.
4. Johannes Blömer, Jorge Guajardo, and Volker Krummel. Provably Secure Masking of AES. In *Selected Areas in Cryptography*, pages 69–83, 2004.
5. Andrey Bogdanov. Multiple-Differential Side-Channel Collision Attacks on AES. In *CHES*, pages 30–44, 2008.
6. David Canright. A Very Compact S-Box for AES. In *CHES*, pages 441–455, 2005.
7. Anne Canteaut, Claude Carlet, Pascale Charpin, and Caroline Fontaine. Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions. In *EUROCRYPT*, pages 507–522, 2000.
8. Claude Carlet. On Highly Nonlinear S-Boxes and Their Inability to Thwart DPA Attacks. In *INDOCRYPT*, pages 49–62, 2005.
9. Joan Daemen and Vincent Rijmen. Rijndael for aes. In *AES Candidate Conference*, pages 343–348, 2000.
10. Julien Doget, Emmanuel Prouff, Matthieu Rivain, and François-Xavier Standaert. Univariate Side Channel Attacks and Leakage Modeling. *J. Cryptographic Engineering*, 1(2):123–144, 2011.
11. Limin Fan, Yongbin Zhou, and Dengguo Feng. A Fast Implementation of Computing the Transparency Order of S-Boxes. *International Conference for Young Computer Scientists*, 0:206–211, 2008.
12. Benedikt Gierlichs, Lejla Batina, Pim Tuyls, and Bart Preneel. Mutual Information Analysis. In *CHES*, pages 426–442, 2008.
13. Jovan Dj. Golic and Christophe Tymen. Multiplicative Masking and Power Analysis of AES. In *CHES*, pages 198–212, 2002.
14. Sylvain Guilley, Philippe Hoogvorst, and Renaud Pacalet. Differential power analysis model and some results. In *CARDIS*, pages 127–142, 2004.
15. Pascal Junod and Serge Vaudenay. Fox : A New Family of Block Ciphers. In *Selected Areas in Cryptography*, pages 114–129, 2004.
16. Paul C. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In *CRYPTO*, pages 104–113, 1996.
17. Kocher P.C., Jaffe J., and Jun B. Differential Power Analysis. In *CRYPTO*, pages 388–397, 1999.
18. Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power Analysis Attacks - Revealing the Secrets of Smart Cards.* Springer, 2007.
19. Stefan Mangard, Norbert Pramstaller, and Elisabeth Oswald. Successfully Attacking Masked AES Hardware Implementations. In *CHES*, pages 157–171, 2005.
20. Mitsuru Matsui. Linear Cryptoanalysis Method for DES Cipher. In *EUROCRYPT*, pages 386–397, 1993.
21. Bodhisatwa Mazumdar, Debdeep Mukhopadhyay, and Indranil Sengupta. Design for Security of Block Cipher S-Boxes to Resist Differential Power Attacks. *International Conference on VLSI Design*, 0:113–118, 2012.
22. Daniel Olejar and Martin Stanek. On cryptographic properties of random boolean functions. *Electronic Journal of Universal Computer Science*, 4:705–717, 1998.
23. Elisabeth Oswald, Stefan Mangard, Norbert Pramstaller, and Vincent Rijmen. A Side-Channel Analysis Resistant Description of the AES S-Box. In *FSE*, pages 413–423, 2005.
24. Enes Pasalic and Subhamoy Maitra. Linear Codes in Generalized Construction of Resilient Functions with Very High Nonlinearity. *IEEE Transactions on Information Theory*, 48(8):2182–2191, 2002.
25. Emmanuel Prouff. DPA Attacks and S-boxes. In *FSE*, pages 424–441, 2005.
26. Jean-Jacques Quisquater and David Samyde. Electromagnetic Analysis (ema): Measures and Counter-Measures for Smart Cards. In *E-smart*, pages 200–210, 2001.
27. Palash Sarkar and Subhamoy Maitra. Nonlinearity Bounds and Constructions of Resilient Boolean Functions. In *CRYPTO*, pages 515–532, 2000.
28. Jennifer Seberry, Xian-Mo Zhang, and Yuliang Zheng. Nonlinearly Balanced Boolean Functions and Their Propagation Characteristics (extended abstract). In *CRYPTO*, pages 49–60, 1993.
29. Claude Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

30. Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. The 128-Bit Blockcipher CLEFIA (Extended Abstract). In Alex Biryukov, editor, *FSE*, volume 4593 of *Lecture Notes in Computer Science*, pages 181–195. Springer, 2007.
31. Carolyn Whitnall and Elisabeth Oswald. A comprehensive evaluation of mutual information analysis using a fair evaluation framework. In *CRYPTO*, pages 316–334, 2011.
32. Amr M. Youssef and Stafford E. Tavares. Information leakage of a randomly selected boolean function. In *Information Theory and Applications'95*, pages 41–52, 1995.
33. Xian-Mo Zhang and Yuliang Zheng. GAC - The Criterion for Global Avalanche Characteristics of Cryptographic Functions. *Journal of Universal Computer Science*, 1:316–333, 1995.

Appendix

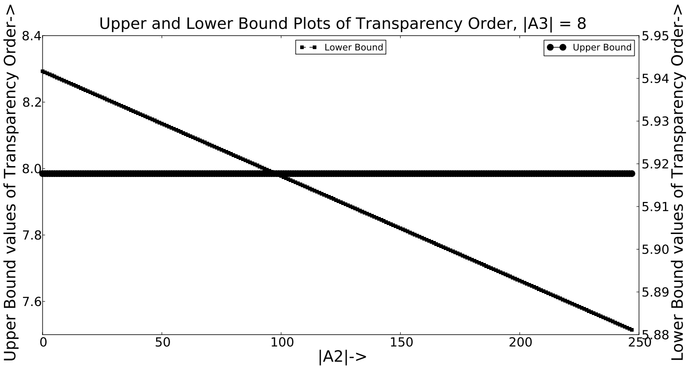

Fig. 4. Lower and Upper Bound plots of *Transparency Order* for S-boxes satisfying $|A_3| = 8$ (or PC of order 1)

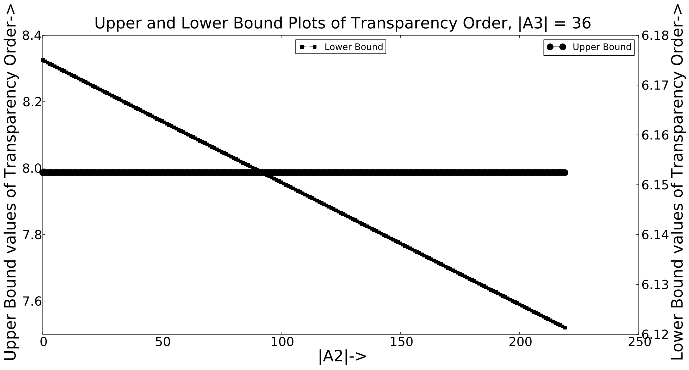

Fig. 5. Lower and Upper Bound plots of *Transparency Order* for S-boxes satisfying $|A_3| = 36$ (or PC of order 2)

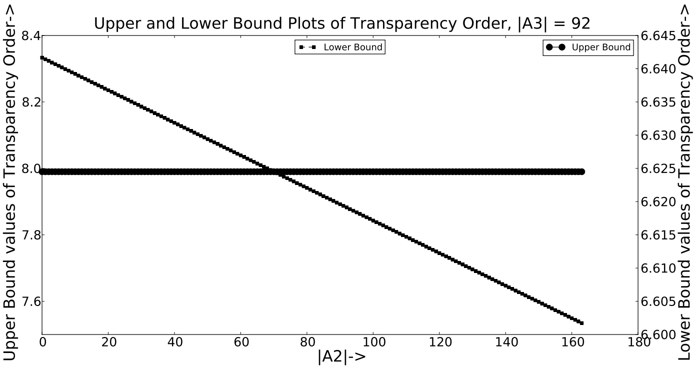

Fig. 6. Lower and Upper Bound plots of *Transparency Order* for S-boxes satisfying $|A_3| = 92$ (or PC of order 3)

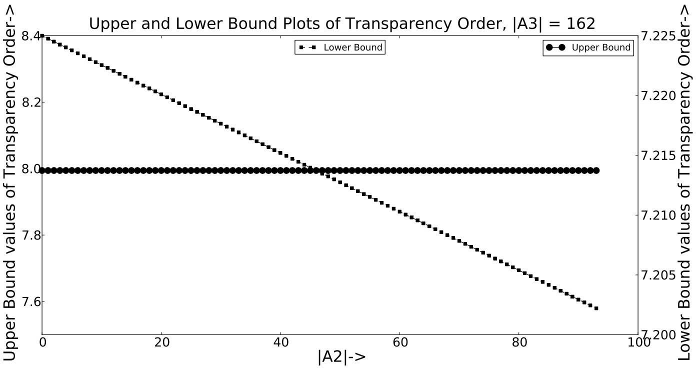

Fig. 7. Lower and Upper Bound plots of *Transparency Order* for S-boxes satisfying $|A_3| = 162$ (or PC of order 4)

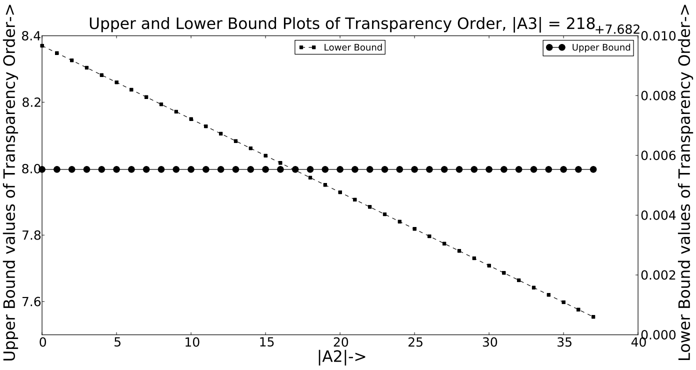

Fig. 8. Lower and Upper Bound plots of *Transparency Order* for S-boxes satisfying $|A_3| = 218$ (or PC of order 5)

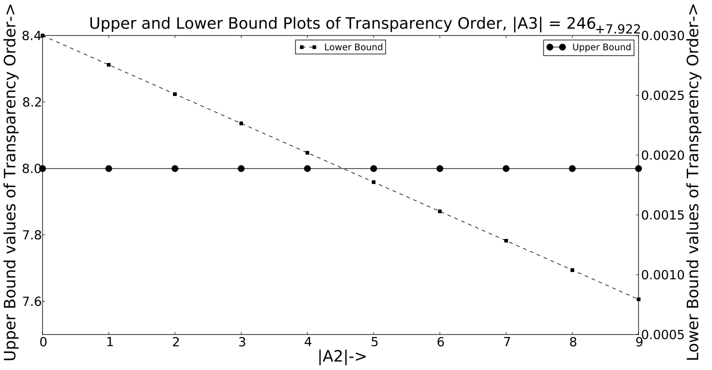

Fig. 9. Lower and Upper Bound plots of *Transparency Order* for S-boxes satisfying $|A_3| = 246$ (or PC of order 6)

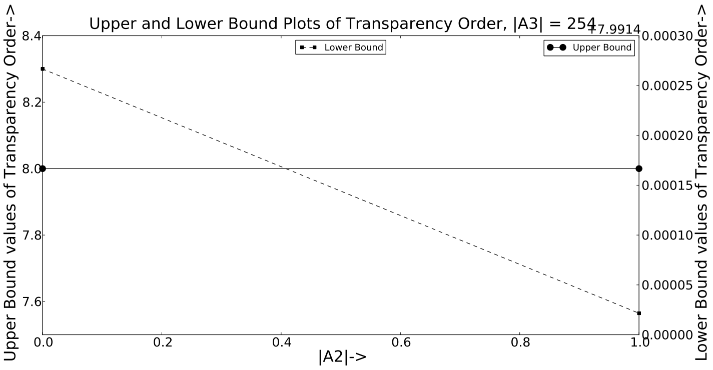

Fig. 10. Lower and Upper Bound plots of *Transparency Order* for S-boxes satisfying $|A_3| = 254$ (or PC of order 7); only two cardinalities of $|A_2|, |A_2| = \{0, 1\}$ exists for this case

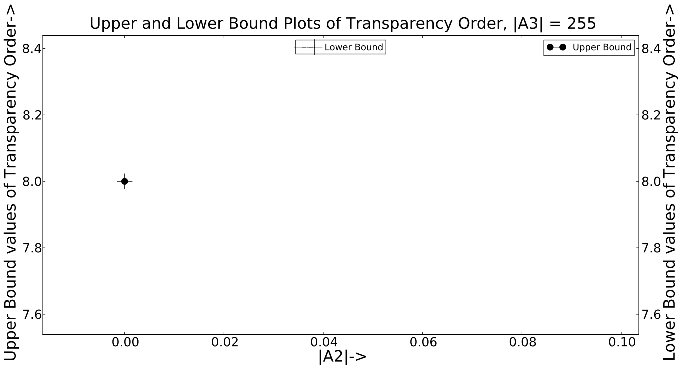

Fig. 11. Lower and Upper bounds of *Transparency Order* for S-boxes satisfying $|A_3| = 255$ (or PC of order 8)

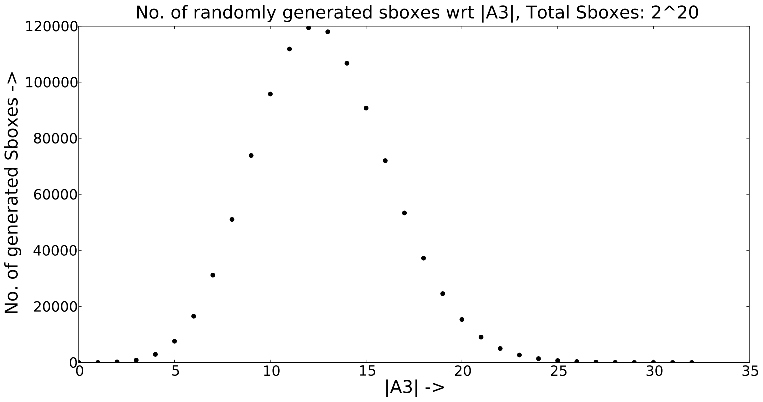

Fig. 12. Normal distribution of randomly generated S-boxes w.r.t. $|A_3|$ in the S-box generation phase

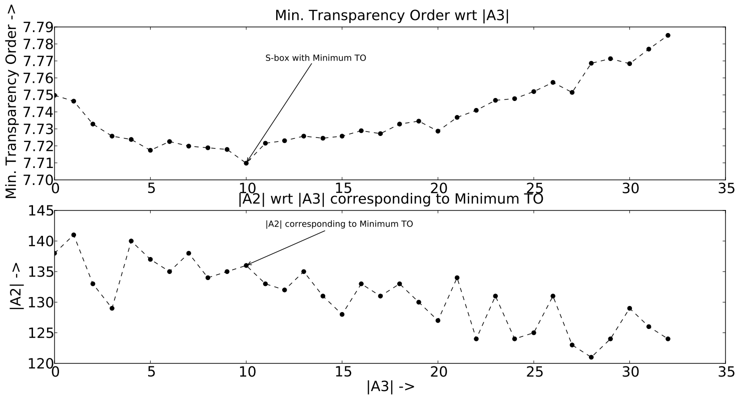

Fig. 13. Minimum *Transparency Order* and corresponding $|A_2|$ vs $|A_3|$ of the generated S-boxes in the S-box generation phase