Transparency Order analysis for $p-ary$ functions

Mayasar Ahmad Dar[1] and Deepmala Sharma[2*]

Department of Mathematics, National Institute of Technology, Raipur, Chhattisgarh, India

Abstract:

Transparency order characterizes the resilience of cryptographic algorithms against DPA attacks in S-boxes. In this paper, we give an upper bound of transparency order for $p-ary$ functions in terms of Walsh-Hadamard transform. The transparency order of $s-plateaued\ p-ary$ functions has been discussed. Finally transparency order and vector concatenation is studied for some important classes of $p-ary$ functions.

Keywords: Transparency order, $p-ary$ functions, Walsh-Hadamard transform.

1. Introduction:

An attempt to quantify the DPA resilience of the S-boxes was made in [1], where the parameter Transparency Order (TO) was introduced. This was an important attempt in defining a metric for the DPA resilience of S-boxes for almost a decade ago. Based on a side-channel efficiency metric close to the standard score measure involved in [2, 4]. E. Prouff [1] tried to explain that S-boxes with smaller transparency order have higher DPA resilience. The transparency order, as defined in [1] was found to depend on the propagation characteristics (PC) of the co-ordinate functions of the S-boxes. The bent functions that satisfy the PC for all orders have been found to have worst transparency order value, while the linear S-boxes have the best DPA resilience. However, the linear S-boxes are not acceptable as a secure cryptographic primitive. Further analyses of TO, as defined in [1], have been followed in [5, 6, 8]. Chakraborty et al. [9] redefined the transparency order as they found some flaws in original definition. The construction of upper and lower bound of transparency order for Boolean functions was investigated [15]. The transparency order of Boolean functions was firstly considered by Picek et al. [7] and some 8-variable Boolean functions with good nonlinearity and relatively good transparency order were found using evolutionary algorithms. In 2015, using similar evolutionary algorithms, Jain and Chaudhari [3] found three 8-variable highly nonlinear balanced Boolean functions that have lower transparency orders than the ones of [7]. In this paper, we extend the work of transparency order from Boolean functions to $p-ary$ functions by giving their tight upper bound of transparency order in terms of Walsh-Hadamard transform. The transparency order of $s-plateaued\ p-ary$ functions has been discussed. Also transparency order in terms of vector concatenation is studied for some classes of $p-ary$ functions.

2. Preliminaries:

Let $\mathbb{F}_p$ and $\mathbb{F}_p^n$ be the prime field of characteristic p and vector space of n-tuples of elements of $\mathbb{F}_p$, respectively. A function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ is called a $p-ary$ function in n variables [10, 14]. The set of all these functions is denoted by $\mathcal{B}_{n,p}$. In particular for $n=2$, $\mathcal{B}_{n,2}$ is the set of

Boolean functions in n variables. The support of $f \in \mathcal{B}_{n,p}$ is defined as $supp(f) = \{x \in \mathbb{F}_p^n : f(x) \neq 0\}$. A function $f \in \mathcal{B}_{n,p}$ is said to be balanced if $|\{x: f(x) = k\}| = p^{n-1}$ for every $k \in \mathbb{F}_p$. The derivative of $f \in \mathcal{B}_{n,p}$ at $x \in \mathbb{F}_p^n$ is defined by $D_u(f)(x) = f(x) - f(x+u)$.
The Walsh-Hadamard transform of $f \in \mathcal{B}_{n,p}$ is defined as

$$W_f(u) = \sum_{x \in \mathbb{F}_p^n} (\xi)^{f(x) - <xu>}$$

where $\xi = e^{2\pi i/p}$ denote the complex pth root of unity and $< xu >$ is the usual inner product in $\mathbb{F}_p^n$. The Walsh-Hadamard Spectrum $\{W_f(u): u \in \mathbb{F}_p^n\}$ of f satisfies the Parseval's identity: [10]

$$\sum_{u \in \mathbb{F}_p^n} |W_f(u)|^2 = p^{2n}$$

A function $f \in \mathcal{B}_{n,p}$ is $p - ary$ bent if $|W_f(u)| = p^{n/2}$ for every $u \in \mathbb{F}_p^n$ [10, 11]. A function $f \in \mathcal{B}_{n,p}$ is called $s - plateaued$ if $|W_f(u)| \in \{0, p^{n+s/2}\}$ for all $u \in \mathbb{F}_p^n$. The case $s = 0$ (respectively $s = 1, 2$) corresponds to $p - ary$ bent (respectively semi-bent) functions and $s = n$ to affine or constant functions. The $p - ary$ semibent functions help to construct to $p - ary$ bent functions [16, 17].
Let $f, g \in \mathcal{B}_{n,p}$ then the sum

$$C_{f,g}(a) = \sum_{x \in \mathbb{F}_p^n} (\xi)^{f(x) - g(x+a)}$$

is the cross-correlation between the function f and g at $a \in \mathbb{F}_p^n$. Moreover for $f = g$, the sum is the autocorrelation of f at a.

The sum-of-squares-of-modulus indicator (SSMI) [15] of $f, g \in \mathcal{B}_{n,p}$ is defined as

$$\sigma_{f,g} = \sum_{a \in \mathbb{F}_p^n} |C_{f,g}(a)|^2$$

The following two corollaries and lemma are used to derive some important theorems.

Corollary 2.1 [12]: Let $f \in \mathbb{F}_p^n$, then for any $y \in \mathbb{F}_p^n$

$$\sum_{x \in \mathbb{F}_p^n} (\xi)^{f(x) - f(x+y)} = \frac{1}{p^n} \sum_{u \in \mathbb{F}_p^n} \xi^{<u,y>} |W_f(u)|^2$$

Corollary 2.2 [12]: For any $v \in \mathbb{F}_p^n$

$$\sum_{y \in \mathbb{F}_p^n} \sum_{x \in \mathbb{F}_p^n} (\xi)^{f(x) - f(x+y) + <v,y>} = p^n |W_f(u)|^2$$

Lemma 2.3[13]: The sum-of squares-of-modulus indicator (SSMI) of $f \in \mathcal{B}_{n,p}$ is given by

$$\sigma_f = \frac{1}{p^n}\sum_{a\in\mathbb{F}_p^n}\left|W_f(a)\right|^4$$

Definition 2.4: For any $u = (u_r, \dots \dots u_1) \in \mathbb{F}_p^r$ and $w = (w_{n-r}, \dots \dots w_1) \in \mathbb{F}_p^{n-r}$, we define vector concatenation as $uw = (u, w) = (u_r, \dots \dots u_1, w_{n-r}, \dots \dots w_1)$.

3. Transparency order of $p-ary$ functions:

By extending the definition of transparency order (TO) of Boolean functions to $p-ary$ functions, the transparency order of $f \in \mathcal{B}_{n,p}$ is given as

$$TO(f) = 1 - \frac{1}{p^n(p^n-1)}\sum_{a\in\mathbb{F}_p^{n*}}\left|\sum_{x\in\mathbb{F}_p^n}(\xi)^{f(x)-f(x+a)}\right| \quad (1)$$

Where $\xi = e^{2\pi i/p}$ denote the complex pth root of unity.
When autocorrelation is zero, then $TO(f) = 1$.
From (1), we compute,

$$\sigma_f \le \left((1-TO(f))p^n(p^n-1)\right)^2 \quad (2)$$

In terms of derivative the transparency order of $f \in \mathcal{B}_{n,p}$ is given by

$$TO(f) = 1 - \frac{1}{p^n(p^n-1)}\sum_{a\in\mathbb{F}_p^{n*}}\left|\sum_{x\in\mathbb{F}_p^n}(\xi)^{D_a(f)(x)}\right|$$

4. Main Results:

The upper bound for transparency order in terms of Walsh-Hadamard transform for $p-ary$ functions, inferring possible relationship between transparency order and Walsh-Hadamard transform, also a connection of transparency order with vector concatenation is discussed.

Theorem 4.1: Let $f \in \mathcal{B}_{n,p}$, then

$$TO(f) \le 1 - \frac{1}{p^{\frac{3n}{2}}(p^n-1)}\left(\sum_{v\in\mathbb{F}_p^n}\left|W_f(v)\right|^4\right)^{\frac{1}{2}}$$

Proof: By Corollary 2.2 for any $v \in \mathbb{F}_p^n$, we have

$$\left(\sum_{y\in\mathbb{F}_p^n}\sum_{x\in\mathbb{F}_p^n}(\xi)^{f(x)-f(x+y)+<v,y>}\right)^2 = p^{2n}\left|W_f(v)\right|^4$$

$$\Rightarrow \sum_{v\in\mathbb{F}_p^n}\left(\sum_{y\in\mathbb{F}_p^n}\sum_{x\in\mathbb{F}_p^n}(\xi)^{f(x)-f(x+y)+<v,y>}\right)^2 = p^{2n}\sum_{v\in\mathbb{F}_p^n}\left|W_f(v)\right|^4$$

Using Lemma 2.3 and (2), we get

$$\frac{1}{p^{3n}}\sum_{v\in\mathbb{F}_p^n}\left(\sum_{y\in\mathbb{F}_p^n}\sum_{x\in\mathbb{F}_p^n}(\xi)^{f(x)-f(x+y)+<v,y>}\right)^2=\sum_{v\in\mathbb{F}_p^n}\left|C_f(v)\right|^2=\sigma_f$$

$$\leq\left((1-TO(f))p^n(p^n-1)\right)^2$$

Therefore, we have

$$p^n\sigma_f\ \leq p^n\left((1-TO(f))p^n(p^n-1)\right)^2$$

$$\Rightarrow\sum_{v\in\mathbb{F}_p^n}\left|W_f(v)\right|^4\leq p^n\left((1-TO(f))p^n(p^n-1)\right)^2$$

$$\Rightarrow TO(f)\leq 1-\frac{1}{p^{\frac{3n}{2}}(p^n-1)}\left(\sum_{v\in\mathbb{F}_p^n}\left|W_f(v)\right|^4\right)^{\frac{1}{2}}$$

and the result follows.

Clearly here the transparency order will be equal to 1 when $\sum_{v\in\mathbb{F}_p^n}\left|W_f(v)\right|^4$ is zero, but this is possible only when autocorrelation sum is zero. The autocorrelation is zero in case of bent function [10], therefore the transparency order of bent function is 1. Also modulus indicator is zero, so $f(x)-f(x-v)$ is balanced.

Theorem 4.2: If f is $s-plateaued\ p-ary$ function, then

$$TO(f)\leq\ 1-\frac{p^{n+s}}{p^{2n}(p^n-1)}\sum_{y\in\mathbb{F}_p^{n*}}\left|\sum_{u\in\mathbb{F}_p^n}(\xi)^{<u,y>+2a}\right|$$

where, $\lambda_f=\{u\in\mathbb{F}_p^n:\left|W_f(u)\right|\neq 0\}$

Proof: We know that

$$TO(f)=\ 1-\frac{1}{p^n(p^n-1)}\sum_{y\in\mathbb{F}_p^{n*}}\left|\sum_{x\in\mathbb{F}_p^n}(\xi)^{f(x+a)-f(x)}\right|$$

Using Corollary 2.1, we have

$$TO(f)=1-\frac{1}{p^{2n}(p^n-1)}\sum_{y\in\mathbb{F}_p^{n*}}\left|\sum_{u\in\mathbb{F}_p^n}(\xi)^{<u,y>}\left|W_f(u)\right|^2\right|$$

But f is $s-plateaued\ p-ary$ function, iff

$$\left|W_f(u)\right|\in\left\{0,\pm p^{\frac{n+s}{2}}\xi^a\right\}\ \text{for some}\ a\in\mathbb{F}_p$$

Using the fact that $\lambda_f = \{u \in \mathbb{F}_p^n : |W_f(u)| \neq 0\}$, we get,

$$TO(f) = 1 - \frac{1}{p^{2n}(p^n - 1)} \sum_{y \in \mathbb{F}_p^{n*}} \left| \sum_{u \in \mathbb{F}_p^n} (\xi)^{<u,y>} \left((p^{\frac{n+s}{2}}) \xi^a \right)^2 \right|$$

$$TO(f) = 1 - \frac{p^{n+s}}{p^{2n}(p^n - 1)} \sum_{y \in \mathbb{F}_p^{n*}} \left| \sum_{u \in \mathbb{F}_p^n} (\xi)^{<u,y>+2a} \right|$$

and the result follows.

Theorem 4.3: Let $f = uw = (u, w) = (u_r, \dots \dots u_1, w_{n-r}, \dots \dots w_1)$ be the vector concatenation of $u = (u_r, \dots \dots u_1) \in \mathbb{F}_p^r$ and $w = (w_{n-r}, \dots \dots w_1) \in \mathbb{F}_p^{n-r}$, then

$$TO(f) = 1 - \frac{1}{p^n(p^n - 1)} \sum_{u,w \in \mathbb{F}_p^{n*}} \left| \sum_{v \in \mathbb{F}_p^r} C_{f_v, f_{v+u}}(w) \right|$$

where, $C_{f_v, f_{v+u}}(w)$ is the autocorrelation of f.

Proof: By lemma 2.3 [13]

$$\sum_{x \in \mathbb{F}_p^n} (\xi)^{f(x) - f(x+uw)} = \sum_{v \in \mathbb{F}_p^r} \sum_{z \in \mathbb{F}_p^{n-r}} \xi^{f_v(z) - f_{(v+u)}(z+w)}$$

$$\Rightarrow \sum_{u,w \in \mathbb{F}_p^{n*}} \left| \sum_{x \in \mathbb{F}_p^n} (\xi)^{f(x) - f(x+uw)} \right| = \sum_{u,w \in \mathbb{F}_p^{n*}} \sum_{v \in \mathbb{F}_p^r} \sum_{z \in \mathbb{F}_p^{n-r}} \left| \xi^{f_v(z) - f_{(v+u)}(z+w)} \right|$$

Using (1) we get

$$\left(1 - TO(f)\right) p^n (1 - p^n) = \sum_{u,w \in \mathbb{F}_p^{n*}} \sum_{v \in \mathbb{F}_p^r} \left| C_{f_v, f_{v+u}}(w) \right|$$

$$TO(f) = 1 - \frac{1}{p^n(p^n - 1)} \sum_{u,w \in \mathbb{F}_p^{n*}} \left| \sum_{v \in \mathbb{F}_p^r} C_{f_v, f_{v+u}}(w) \right|$$

and the result follows.

Lemma 4.1: Two $p - ary$ functions f and g are said to have complementary transparency order iff $TO(f_u) + TO(g_u) = 2$ for all $u \in \mathbb{F}_p^{n*}$

Proof: We know that two functions f and g have complementary autocorrelation iff for all $u \in \mathbb{F}_p^n$

$$C_f(u) + C_g(u) = 0$$

$$\Rightarrow \sum_{u \in \mathbb{F}_p^{n*}} |C_f(u)| + \sum_{u \in \mathbb{F}_p^{n*}} |C_g(u)| = 0$$

$$\Rightarrow (1 - TO(f_u))p^n(p^n - 1) + (1 - TO(g_u))p^n(p^n - 1) = 0$$

$$\Rightarrow TO(f_u) + TO(g_u) = 2$$

Theorem 4.4:

Let $f_1 \in \mathcal{B}_{r,p}$ and $f_2 \in \mathcal{B}_{s,p}$ then the transparency order of a function $g \in \mathcal{B}_{r+s,q}$ expressed as

$$g(x_{r+s}, \dots \dots x_{r+1}, x_r, \dots \dots x_1) = f_1(x_r, \dots \dots x_1) + f_2(x_{r+s}, \dots \dots x_{r+1})$$

is given by

$$TO(g) \leq 1 - \frac{|W_{f_1}(u)W_{f_2}(v)|^2 - p^n}{(p^n - 1)} \qquad where\ \ n = r + s$$

Proof: Let $(u, v) \in \mathbb{F}_p^r \times \mathbb{F}_p^s$ then

$$W_g(u, v) = \sum_{(u,v) \in \mathbb{F}_p^r \times \mathbb{F}_p^s} (\xi)^{g(x,y) + <u,x> + <v,y>} = W_{f_1}(u).W_{f_2}(v)$$

$$|W_g(u, v)|^2 = |W_{f_1}(u).W_{f_2}(v)|^2$$

Using Corollary 2.2, we have

$$\sum_{(u,v) \in \mathbb{F}_p^{r*} \times \mathbb{F}_p^{s*}} \left| \sum_{x \in \mathbb{F}_p^r} (\xi)^{f(x) - f(x+uv)} \right| = p^n |W_g(u, v)|^2 = p^n |W_{f_1}(u).W_{f_2}(v)|^2$$

$$\geq p^n |W_{f_1}(u).W_{f_2}(v)|^2 - p^{2n}$$

In the above equation $n = r + s$

Using (1), we get

$$(1 - TO(g))(p^n - 1) \geq |W_{f_1}(u).W_{f_2}(v)|^2 - p^n$$

$$TO(f) \leq 1 - \frac{|W_{f_1}(u).W_{f_2}(v)|^2 - p^n}{(p^n - 1)}$$

and the result follows.

In particular if $f_1 \in \mathcal{B}_{r,p}$ and $f_2 \in \mathcal{B}_{s,p}$ are bent functions then $g \in \mathcal{B}_{r+s,q}$ is also bent, as it is clear from above that transparency order of $g \in \mathcal{B}_{r+s,q}$ is 1 , because $\left|W_{f_1}(u)\right| = p^{\frac{r}{2}}$ and $\left|W_{f_2}(v)\right| = p^{\frac{s}{2}}$ which implies $TO(g) = 1\ \forall (u,v) \in \mathbb{F}_p^r \times \mathbb{F}_p^s$. Next we show that if $g \in \mathcal{B}_{r+s,q}$ has transparency order equal 1 , then $f_1 \in \mathcal{B}_{r,p}$ and $f_2 \in \mathcal{B}_{s,p}$ are bent functions. Suppose that f_1 is not $p-ary$ bent then $\exists\ u \in \mathbb{F}_p^r$ such that $\left|W_{f_1}(u)\right| > p^{\frac{r}{2}}$ this implies that $\left|W_{f_1}(u)\right| < p^{\frac{s}{2}}$ for every $v \in \mathbb{F}_p^s$ as, $1 \leq 1 - \frac{\left|W_{f_1}(u).W_{f_2}(v)\right|^2 - p^n}{(p^n - 1)}$. This contradicts the fact that $\sum_{v \in \mathbb{F}_p^s} \left|W_{f_2}(v)\right|^2 = p^s$.

5. Conclusion:

For the first time, the notion of transparency order of $p-ary$ function is discussed, we give some bounds between Walsh-Hadamard transform and transparency order inferring possible relationship between transparency order and Walsh-Hadamard transform, it is found that $p-ary$ bent function has the upper bound of transparency order. The result is extended to $s-plateaued\ p-ary$ function. Also transparency order in terms of vector concatenation is discussed for some important classes of $p-ary$ functions. Future scope of the work is to construct some more classes of $p-ary$ functions in terms of nonlinearity. The open problems like , what is the minimum value of transparency order for a particular nonlinear $p-ary$ function, how to construct low transparency order $p-ary$ functions with maximum nonlinearity, how to correlate the work on transparency order of $p-ary$ functions with cryptanalysis are deserving to be discussed.

Remark: Some of the results of this paper were presented at the International Conference on Fundamental and Applied Sciences (ICFAS 2021) organized by Faculty of Sciences and I.Q.A.C. Bharatiya Vidya Bhavan's Hazarimal Somani College of Arts and Science, Mumbai from 24th March 2021 to 26th March 2021.

References:

1. E. Prou. 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.
2. 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.
3. P. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In M. Wiener, editor, CRYPTO '99, volume 1666 of LNCS, pages 388–397. Springer, 1999.
4. C. Whitnall and E. Oswald. A Comprehensive Evaluation of Mutual Information Analysis Using a Fair Evaluation Framework. In P. Rogaway, editor, CRYPTO, volume 6841 of Lecture Notes in Computer Science, pages 316-334. Springer, 2011.
5. 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.
6. M. A. Evci and S. Kavut. DPA Resilience of Rotation-Symmetric S-boxes. In IWSEC, pages 146-157, 2014.
7. S. Picek , L. Batina , D. Jakobovic : Evolving DPA-Resistant Boolean Functions, PPSN 2014, LNCS 8672, pp. 812-821. Springer, Berlin, 2014.
8. 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.
9. K. Chakraborty , S. Sarkar, S. Maitra, B. Mazumdar, D. Mukhopadhyay , E. Prou. : Redefining the transparency order. Des. Codes Cryptogr. 82, 95-115, 2017.
10. P.V. Kumar, R.A. Scholtz and L.R. Welch, Generalized bent functions and their properties. Journal of Combinatorial Theory, Ser. A 1(40), pp. 90-107, 1985.
11. O.S. Rothaus, On bent functions. Journal of Combinatorial Theory 20 , pp. 300-305, 1976.
12. D. Singh, M. Bhaintwal, and B.K Singh, Some properties of q-ary functions based on spectral analysis, Int. J. Comput. Maths, 2013.
13. D. Singh, M. Bhaintwal, and B.K Singh, Some results on q-ary bent functions, Int. J. Comput. Math . 90(9), pp. 1761-1773, 2013.
14. M. Bimal, S. Pantelimon, G. Suganta, New classes of p-ary bent functions, cryptogr. commun. 11 pp. 77-92, 2019.
15. Q. Wang, P. Stanica, Transparency Order for Boolean functions: analysis and construction", Des. Codes Cryptogr. https://doi.org/10.1007/s10623-019-00604-1, 2018.
16. A. Cesmelioglu and W. Meidl, Bent functions of maximal degree, IEEE Trans. Inf. Theory 58(2), pp. 1186-1190, 2012.
17. A. Cesmelioglu and W. Meidl, A construction of bent functions from plateaued functions, Des.Codes Cryptogr. 66, pp. 231-242, 2013.