Mathematics and Statistics 10(6): 1320-1325, 2022
DOI: 10.13189/ms.2022.100618 http://www.hrpub.org

Transparency Order and Cross-Correlation Analysis of Boolean Functions

Mayasar Ahmad Dar[1], **Hiral Raja**[2], **Afshan Butt**[3], **Deepmala Sharma**[1,*]

[1]Department of Mathematics, National Institute of Technology, Raipur(C.G)-492010, India
[2]Department of Mathematics, Dr. C. V. Raman University, Kota Bilaspur, India
[3]Department of Mathematics, Bhilai Institute of Technology, Raipur, India

Received July 7, 2022; Revised October 18, 2022; Accepted October 25, 2022

Cite This Paper in the following Citation Styles

***(a)**: [1] Mayasar Ahmad Dar, Hiral Raja, Afshan Butt, Deepmala Sharma, "Transparency Order and Cross-Correlation Analysis of Boolean Functions," Mathematics and Statistics, Vol.10, No.6, pp. 1320-1325, 2022. DOI: 10.13189/ms.2022.100618*

***(b)**: Mayasar Ahmad Dar, Hiral Raja, Afshan Butt, Deepmala Sharma (2022). Transparency Order and Cross-Correlation Analysis of Boolean Functions. Mathematics and Statistics, 10(6), 1320-1325. DOI: 10.13189/ms.2022.100618*

Abstract Transparency order is considered to be a cryptographically significant property that characterizes the resistance of S-boxes in opposition to differential power analysis attacks. The S-box having low transparency order is more resistant to these attacks. Until now, little attempts have been noticed to examine theoretically the transparency order and its relationship with other cryptographic properties. All constructions associated with transparency order are relying on search algorithms. In this paper, we discuss the new interpretation of bent functions in terms of their transparency order. Using the concept of vector concatenation and correlation characteristics, we find the transparency order of Boolean functions. The notion of complementary transparency order is given. For a pair of Boolean functions, we interpret complementary transparency order by their Walsh-Hadamard transform. We establish a relationship of transparency order with cross-correlation for a pair of Boolean functions. We find a relationship of transparency order with $(n-2)-$variable decomposition bent functions. We generalize the bounds on sum-of-squares of autocorrelation in terms of transparency order of Boolean functions using Walsh-Hadamard spectra. Further the transparency order of a function fulfilling the propagation criterion about a linear subspace is evaluated.

Keywords Transparency order, Cross-Correlation, Boolean functions, Walsh-Hadamard Transform

1 Introduction

The basic nonlinear component of S-boxes in block and stream ciphers is investigated in two ways. One way is to examine the cryptographic properties on the basis of nonlinearity, algebraic immunity, correlation immunity, propagation criteria etc. and the other way is to examine the cryptographic properties through differential power analysis (DPA) with indicators like transparency order, Signal-to-Noise Ratio, confusion coefficient etc. Side-channel analysis is considered as an effective approach in which block ciphers are attacked [10]. DPA [9] is a kind of Side-channel analysis, which deals with the study of utilization of power in cryptographic hardware device. DPA is regarded more able than the differential or linear cryptanalysis [3, 14]. The cryptographic properties of S-box (the only nonlinear part in many ciphers) should be good. To assess the functioning of an S-box in opposition to Side-channel analysis, various properties were suggested. Signal-to-Noise Ratio [13] was introduced in 2004 as the first property related with Side-channel analysis. Prouff [6] suggested the idea of transparency order which depicts the resistance of Boolean functions to DPA attacks. Some countermeasures like hiding and masking schemes [14] are used to resist DPA attacks. Using evolutionary algorithms, some multi-variable Boolean functions having high nonlinearity and low transparency order were constructed [15, 2]. Chakraborty et al.[7] revised the transparency order definition and proposed that a low transparency order is needed to counter these attacks as they found some flaws in the original definition. They verified that the revised definition has an effect on the resistance of the execution in opposition to DPA attacks. Wang and Stanica [12] gave bounds of transparency order in connection with nonlinearity, also they

showed that transparency order and nonlinearity both are not good simultaneously for certain classes of Boolean functions. They constructed some classes of Boolean functions with comparatively suitable transparency order.

DPA is also considered to be a threat in case of stream ciphers. A DPA attack was performed by using nonlinear part of Grain on the cipher [16]. In case of stream ciphers, filter generator and nonlinear combiner are two well known models [4]. The only nonlinear part in these models is the Boolean function having significant cryptographic properties. It is important to note that if all other cryptographically significant properties of some Boolean functions are equal, then a planner chooses the function having low transparency order. In this paper, we discuss the cross-correlation and new characterization of Boolean functions via their transparency order. Here we find some results of transparency order of Boolean functions based on vector concatenation. We introduce the concept of complementary transparency order and evaluate some results of bent functions with complementary transparency order and nonlinearity. A relationship of transparency order with $(n-2)$ variable decomposition bent function is established. Finally, we evaluate the bounds on sum of squares of autocorrelation and functions satisfying propagation criterion in terms of their transparency order.

1.1 Definitions and Notations

Let $\mathbb{F}_2$ be the finite field and $\mathbb{F}_2^n$ be the vector space of all $n-$tuples over $\mathbb{F}_2$. A function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is known as $n-$variable Boolean function and the set of all these functions is denoted by $\mathcal{B}_{n,2}$. The support of a Boolean function f is defined by $S_f = \{x \in \mathbb{F}_2^n : f(x) \neq 0\}$, whose cardinality $\mid S_f \mid$ is known as the *Hamming weight* of f. The *Hamming distance* $d(f,g)$ between $f, g \in \mathcal{B}_{n,2}$ is the number of elements $x \in \mathbb{F}_2^n$ where these functions differ. For a vector $x = (x_1, x_2, ..., x_n)$, the *Hamming weight* denoted by $wt(x)$, is the number of x_i, such that $x_i \neq 0$. A Boolean function of $n-$variable with degree 1 is known as *affine* and $\mathcal{A}_n$ is used to denote the set of all these functions. The derivative of $f, g \in \mathcal{B}_{n,2}$ at $t \in \mathbb{F}_2^n$ is defined as $D_{f,g}(t) = f(x) + g(x+t)$; and for $f = g$, $D_f(t) = f(x) + f(x+t)$ is derivative of f at $t \in \mathbb{F}_2^n$.

The Walsh-Hadamard transform of $f \in \mathcal{B}_{n,2}$ at $e \in \mathbb{F}_2^n$ is given by

$$W_f(e) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\langle e,x \rangle},$$

where $\langle e, x \rangle$ is the usual inner product in $\mathbb{F}_2^n$.

Here the Walsh spectrum only gives integer values.

The *nonlinearity* of $f \in \mathcal{B}_{n,2}$, denoted by $nl(f)$, is the minimum distance between f and $\mathcal{A}_n$. The *nonlinearity* of f is also defined as

$$nl(f) = 2^{n-1} - \frac{1}{2} max_{e \in \mathbb{F}_2^n} \mid W_f(e) \mid .$$

An function $f \in \mathcal{B}_{n,2}$ is *bent*, if its nonlinearity is $2^{n-1} - 2^{\frac{n}{2}-1}$. These types of Boolean functions are of specific importance in cryptography.

Let $f, g \in \mathcal{B}_{n,2}$, then the sum

$$C_{f,g}(e) = \sum_{x \in \mathbb{F}_p^n} (-1)^{f(x)+g(x+e)}$$

is the cross-correlation between f and g at $e \in \mathbb{F}_2^n$. Furthermore for $f = g$, the sum $C_f(e)$ is called the auto-correlation of f at e.

The sum-of-squares-of-modulus indicator of $f, g \in \mathcal{B}_{n,2}$ is given by

$$\sigma_{f,g} = \sum_{e \in \mathbb{F}_2^n} C_{f,g}^2(e).$$

Let $f = (f_1, f_2, ..., f_m)$ be a vectorial function from $\mathbb{F}_2^n \to \mathbb{F}_2^m$. The *transparency order* of f is given by [7]

$$\mathcal{TO}(f) = \max_{\gamma \in \mathbb{F}_2^m} \left(m - \frac{1}{2^{2n}-2^n} \sum_{e \in \mathbb{F}_2^{n*}} \sum_{j=1}^{m} \left| \sum_{i=1}^{m} (-1)^{\gamma_i + \gamma_j} C_{f_i,f_j}(e) \right| \right),$$

where $C_{f_i,f_j}(e)$ is the cross-correlation between f_i and f_j. Also $\mathbb{F}_2^{n*} = \mathbb{F}_2^n - \{0\}$ and $f_i, f_j \in \mathcal{B}_{n,2}$.

If $m = 1$, then the *transparency order* of $f \in \mathcal{B}_{n,2}$ is given by

$$\mathcal{TO}(f) = 1 - \frac{1}{2^n(2^n-1)} \sum_{e \in \mathbb{F}_2^{n*}} |C_f(e)| . \tag{1}$$

Any two pairs of $n-$variable Boolean functions $(g_1(x), g_2(x)), (g_3(x), g_4(x))$ are said to be *perfectly uncorrelated* if $C_{g_1,g_2}(e) C_{g_3,g_4}(e) = 0 \ \forall \ e \in \mathbb{F}_2^n$ and are said to be uncorrelated of degree t if $C_{g_1,g_2}(e) C_{g_3,g_4}(e) = 0 \ \forall \ e \in \mathbb{F}_2^n$ such that $0 \leq wt(e) \leq t$.

It should be remembered that in case of Boolean functions the redefined transparency order is same as the original one [6].

The below given lemma that will be used afterwards is the consequence of Lemma 2.2 [12].

Lemma 1: Let $f \in \mathcal{B}_{n,2}$ then for any $v \in \mathbb{F}_2^n$

$$\sum_{y \in \mathbb{F}_2^{n*}} \mid C_f(y) \mid \geq |W_f^2(v) - 2^n|.$$

Proof. By Lemma 2.2 [12], for any $v \in \mathbb{F}_2^n$, we have

$$\begin{aligned} \sum_{y \in \mathbb{F}_2^{n*}} \mid C_f(y) \mid &= \sum_{y \in \mathbb{F}_2^{n*}} \left| (-1)^{\langle v,y \rangle} C_f(y) \right| \\ &\geq \left| \sum_{y \in \mathbb{F}_2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+y)+\langle v,y \rangle} - 2^n \right| \\ &= |W_f^2(v) - 2^n|. \end{aligned}$$

□

From Lemma 1 and equation (1) we compute

$$W_f^2(v) \leq (1 - \mathcal{TO}(f)) 2^n (2^n - 1) + 2^n \tag{2}$$

The upper bound for the above relations is obtained in case of bent function.

2 New Interpretation of Bent Functions via Transparency Order

In our next results we give a new interpretation of Boolean functions by using correlation characteristics of its sub-functions. This may be viewed as the new depiction of bent functions presented in [11].
Let $v = (v_r, ..., v_1)$, we define

$$f_v(x_{n-r}, ..., x_1) = f(x_n = v_r, ..., x_{n-r+1} = v_1, x_{n-r}, ..., x_1).$$

For any $c = (c_r, ...c_1) \in \mathbb{F}_2^r$ and $d = (d_{n-r}, ...d_1) \in \mathbb{F}_2^{n-r}$ vector concatenation is defined as

$$cd = (c, d) = (c_r, ...c_1, d_{n-r}, ...d_1).$$

Theorem 2.1. *Let $c \in \mathbb{F}_2^r$, $d \in \mathbb{F}_2^{n-r}$ and $f \in \mathcal{B}_{n,2}$, then*

$$\mathcal{TO}(f_{cd}) = 1 - \tfrac{1}{2^n(2^n-1)} \sum_{(c,d)\in\mathbb{F}_2^{n*}} \left| \sum_{v\in\mathbb{F}_2^r} C_{f_v, f_{v+c}}(d) \right|.$$

Proof. For $c \in \mathbb{F}_2^r$ and $d \in \mathbb{F}_2^{n-r}$, we have

$$\begin{aligned}
\mathcal{TO}(f_{cd}) &= 1 - \frac{1}{2^n(2^n-1)} \sum_{(c,d)\in\mathbb{F}_2^{n*}} |C_f(cd)| \\
&= 1 - \frac{1}{2^n(2^n-1)} \sum_{(c,d)\in\mathbb{F}_2^{n*}} \left| \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+f(x+cd)} \right| \\
&= 1 - \frac{1}{2^n(2^n-1)} \\
&\quad \sum_{(c,d)\in\mathbb{F}_2^{n*}} \left| \sum_{v\in\mathbb{F}_2^r} \sum_{z\in\mathbb{F}_2^{n-r}} (-1)^{f(vz)+f(vz+cd)} \right|.
\end{aligned}$$

Here we write vector x as the vector concatenation of strings v and z. For a fixed v we have $f(vz) = f_v(z)$ and $f(vz + cd) = f_{v+c}(z + d)$. This gives

$$\begin{aligned}
\mathcal{TO}(f_{cd}) &= 1 - \frac{1}{2^n(2^n-1)} \\
&\quad \sum_{(c,d)\in\mathbb{F}_2^{n*}} \left| \sum_{v\in\mathbb{F}_2^r} \sum_{z\in\mathbb{F}_2^{n-r}} (-1)^{f_v(z)+f_{v+c}(z+d)} \right| \\
&= 1 - \frac{1}{2^n(2^n-1)} \sum_{(c,d)\in\mathbb{F}_2^{n*}} \left| \sum_{v\in\mathbb{F}_2^r} C_{f_v, f_{v+c}}(d) \right|,
\end{aligned}$$

where $\sum_{v\in\mathbb{F}_2^r} C_{f_v, f_{v+c}}(d)$ is the auto-correlation of f.
Hence the result follows. □

Corollary 2.2. *Let $f \in \mathbb{F}_2^n$ and f_0 and f_1 be obtained from f by respectively confining the variable x_n to 0 and 1 , then we can write*

(i) $\mathcal{TO}(f_{cd}) = 1 - \frac{1}{2^n(2^n-1)} \sum_{(0,d)\in\mathbb{F}_2^{n*}} |C_f(0d)|$
$= 1 - \frac{1}{2^n(2^n-1)} \sum_{(0,d)\in\mathbb{F}_2^{n*}} |C_{f_0}(d) + C_{f_1}(d)|.$

(ii) $\mathcal{TO}(f_{cd}) = 1 - \frac{1}{2^n(2^n-1)} \sum_{(1,d)\in\mathbb{F}_2^{n*}} |C_f(1d)|$
$= 1 - \frac{1}{2^n(2^n-1)} \sum_{(1,d)\in\mathbb{F}_2^{n*}} |C_{f_0.f_1}(d) + C_{f_1,f_0}(d)|$
$= 1 - \frac{2}{2^n(2^n-1)} \sum_{(1,d)\in\mathbb{F}_2^{n*}} |C_{f_0.f_1}(d)|.$

Any two bent functions $f, g \in \mathcal{B}_{n,2}$ have complementary transparency order if and only if $\mathcal{TO}(f_u) + \mathcal{TO}(g_u) = 2$ for all $u \in \mathbb{F}_2^{n*}$. In the below given theorem, we give the complementary transparency order through Walsh-Hadamard transform.

Theorem 2.3. *Any two bent functions f and g on $\mathbb{F}_2^n$ have complementary transparency order if*

$$W_f^2(v) + W_g^2(v) = 2^{n+1} \ \forall \ v \in \mathbb{F}_2^n.$$

Proof. Suppose $f, g \in \mathcal{B}_{n,2}$ possess complementary transparency order, then using Lemma 1, we get

$$\begin{aligned}
W_f^2(v) + W_g^2(v) &= 2^{n+1} + \sum_{y\in\mathbb{F}_2^{n*}} | C_f(y) | + \sum_{y\in\mathbb{F}_2^{n*}} | C_g(y) | \\
&= 2^{n+1}.
\end{aligned}$$

Conversely suppose that $W_f^2(v) + W_g^2(v) = 2^{n+1} \ \forall \ v \in \mathbb{F}_2^n$, then

$$\begin{aligned}
\mathcal{TO}(f) + \mathcal{TO}(g) &= 1 - \frac{1}{2^n(2^n-1)} \sum_{y\in\mathbb{F}_2^{n*}} | C_f(y) | \\
&\quad + 1 - \frac{1}{2^n(2^n-1)} \sum_{y\in\mathbb{F}_2^{n*}} | C_g(y) | \\
&= 2 - \frac{1}{2^n(2^n-1)} \Big(\sum_{y\in\mathbb{F}_2^{n*}} | C_f(y) | \\
&\quad + \sum_{y\in\mathbb{F}_2^{n*}} | C_g(y) | \Big) \\
&= 2 - \frac{1}{2^n(2^n-1)} \big(W_f^2(v) + W_g^2(v) - 2^{n+1} \big) \\
&= 2.
\end{aligned}$$

Therefore f and g have complementary transparency order. Hence the result follows.

Furthermore for two bent functions f and g, we have $W_f(v) = 2^n - 2^n nl(f)$ and $W_g(v) = 2^n - 2^n nl(g)$ respectively. Using these values of $W_f(v)$ and $W_g(v)$ in Theorem 2.3, we compute

$$nl^2(f) + nl^2(g) = 2^{n-1} + 2^n(nl(f) + nl(g)) - 2^{2n-1}.$$

Therefore we may also write $nl^2(f) + nl^2(g) = 2^{n-1} + 2^n(nl(f) + nl(g)) - 2^{2n-1}$, if f and g have

complementary transparency order.

□

Theorem 2.4. *Let k be an $(n+1)-$variable function and n is an odd integer such that*

$$k(y_{n+1}, y_n, ..., y_1) = (1+y_{n+1})f(y_n, ..., y_1)+y_{n+1}g(y_n, ..., y_1)$$

Then the below given statements are equivalent
(i) k is bent.
(ii) f and g have complementary transparency order.
(iii) $C_{f,g}(u) = 0$ and $nl(f) = nl(g) = 2^{n-1} - 2^{\frac{n-1}{2}}$

Proof. (i)⇒(ii) Let k be bent, then $\mathcal{TO}(k) = 1$ for all nonzero $t \in \mathbb{F}_2^{n+1}$. Let u be any vector in $\mathbb{F}_2^{n*}$. Applying Corollary 4.1[11], we obtain

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

Since $u \neq 0$, we have $C_k(0u) = 0$, therefore $C_f(u)+C_g(u) = 0$. This gives

$$\mathcal{TO}(f) + \mathcal{TO}(g) = 2.$$

Thus f and g have complementary transparency order.
(ii)⇒(i) is obvious from above.
(ii)⇒(iii) Suppose that $\mathcal{TO}(f) + \mathcal{TO}(g) = 2$, for all $v \in \mathbb{F}_2^n$, then from Theorem 2.3, we have $W_f^2(v) + W_g^2(v) = 2^{n+1}$. Now using Jacob's lemma [8], we get either $W_f^2(u) = 2^{n+1}$ and $W_g^2(u) = 0$ or $W_f^2(u) = 0$ and $W_g^2(u) = 2^{n+1}$. In either case $W_f(u)W_g(u) = 0$, therefore, f and g have non-intersecting spectra. But two functions have non-intersecting spectra if and only if $C_{f,g}(u) = 0$ for all $u \in \mathbb{F}_2^n$, that means f and g are perfectly uncorrelated. Clearly, $nl(f) = nl(g) = 2^{n-1} - 2^{\frac{n-1}{2}}$. Resilient functions with high nonlinearity are constructed using functions with disjoint spectra [5].
(iii)⇒(i) Proved in Theorem 4.2 [11].

□

3 Transparency Order and Cross-Correlation Theorem

In the below given theorem we give a relationship of Transparency Order with Cross-Correlation Theorem[11].

Theorem 3.1. *If $h, r \in \mathcal{B}_{n,2}$ and $u, y \in \mathbb{F}_2^n$, then*

$$\sum_{u\in\mathbb{F}_2^n} C_{h,r}(u)(-1)^{\langle u,y\rangle}$$

$$\leq 2^n(2^n-1)\sqrt{\left(\frac{2^n}{2^n-1} - \mathcal{TO}(h)\right)\left(\frac{2^n}{2^n-1} - \mathcal{TO}(r)\right)}.$$

Proof. Let $u, y \in \mathbb{F}_2^n$, then from Cross-Correlation Theorem[11]

$$\sum_{u\in\mathbb{F}_2^n} C_{h,r}(u)(-1)^{\langle u,y\rangle} = W_h W_r.$$

Using (2) in above, we compute

$$\left(\sum_{u\in\mathbb{F}_2^n} C_{h,r}(u)(-1)^{\langle u,y\rangle}\right)^2$$
$$\leq \left[(1-\mathcal{TO}(h))2^n(2^n-1)+2^n\right]\left[(1-\mathcal{TO}(r))2^n(2^n-1)+2^n\right]$$
$$= 2^{2n}(2^n-1)^2\left(\frac{2^n}{2^n-1} - \mathcal{TO}(h)\right)\left(\frac{2^n}{2^n-1} - \mathcal{TO}(r)\right).$$

Therefore,

$$\sum_{u\in\mathbb{F}_2^n} C_{h,r}(u)(-1)^{\langle u,y\rangle}$$
$$\leq 2^n(2^n-1)\sqrt{\left(\frac{2^n}{2^n-1} - \mathcal{TO}(h)\right)\left(\frac{2^n}{2^n-1} - \mathcal{TO}(r)\right)}.$$

Hence the result follows. □

When $h = r$, we obtain the below given Corollary.

Corollary 3.2. *If $h \in \mathcal{B}_{n,2}$ and $u, y \in \mathbb{F}_2^n$, then*

$$\sum_{u\in\mathbb{F}_2^n} C_h(u)(-1)^{\langle u,y\rangle} \leq 2^n(2^n-1)\left(\frac{2^n}{2^n-1} - \mathcal{TO}(h)\right).$$

Remark(i): If $\left(\frac{2^n}{2^n-1} - \mathcal{TO}(h)\right)\left(\frac{2^n}{2^n-1} - \mathcal{TO}(r)\right) > 0$ and $\mathcal{TO}(h) < \mathcal{TO}(r)$, then

$$\mathcal{TO}(h) > \frac{2^n}{2^n-1} \quad or \quad \mathcal{TO}(r) < \frac{2^n}{2^n-1}.$$

The below given theorem is the inference of the Theorem 20[19] in a modified form in terms of transparency order by using sum-of-squares-of-modulus indicator. Theorem 20 [19] has various other cryptographic constituents having similar cryptographic characteristics.

Theorem 3.3. *Let $g(s_n, s_{n-1}, s) = (s_n + 1)(s_{n-1} + 1)g_1(s) + (s_n + 1)s_{n-1}g_2(s) + s_n(s_{n-1})g_3(s) + s_n s_{n-1}g_4(s)$; $s_n, s_{n-1} \in \mathbb{F}_2^n, s \in \mathbb{F}_2^{n-2}$. If $(g_1(s), g_2(s))$ and $(g_3(s), g_4(s))$ are perfectly uncorrelated $(n-2)$ variable bent functions then:*

$$\mathcal{TO}(g) \leq 1 - \frac{\sqrt{5\times 2^{2n-1}}}{2^n(2^n-1)}.$$

Proof. Since here in this case[19]

$$\sigma_g = \sigma_{g_1} + \sigma_{g_2} + \sigma_{g_3} + \sigma_{g_4} + 6\sum_{1\leq i<j\leq 4}\sigma_{g_i,g_j} + 24\sum_{a\in\mathbb{F}_2^{n-2}} C_{g_1,g_2}(a)C_{g_3,g_4}(a).$$

It is well known that $\sigma_{g_i,g_j} = 2^{2(n-2)}$ is satisfied by any two bent functions g_i, g_j such that $1 \leq i \neq j \leq 4$. Also the functions are perfectly uncorrelated, so we can write.

$$\sigma_g = 40 \times 2^{2(n-2)} + 0$$

$$\sigma_g = 40 \times 2^{2(n-2)}.$$

But

$$\sigma_g \leq ((1-\mathcal{TO}(g))2^n(2^n-1))^2.$$

Thus we have

$$5\times 2^{2n-1} \leq ((1-\mathcal{TO}(g))2^n(2^n-1))^2.$$

$$\Rightarrow \mathcal{TO}(g) \leq 1-\frac{\sqrt{5\times 2^{2n-1}}}{2^n(2^n-1)}.$$

Hence the result follows. □

Using this theorem , we determine the transparency order of various Boolean functions in $n-$variables.

The preposition 3.1 [11] can be written in a generalized version in the following form. Also we evaluate this result in terms of transparency order.

Proposition 3.4. *Let $f,h \in \mathcal{B}_{n,2}$, then*

$$\sum_{y\in\mathbb{F}_2^n}\Big(\sum_{u\in\mathbb{F}_2^n} C_{f,h}(u)(-1)^{\langle u,y\rangle}\Big)^2 \leq 2^{4n}.$$

Proof. We know that

$$\sum_{u\in\mathbb{F}_2^n} C_{f,h}(u)(-1)^{\langle u,y\rangle} = W_f(y)W_h(y)$$

$$\Rightarrow \sum_{y\in\mathbb{F}_2^n}\Big(\sum_{u\in\mathbb{F}_2^n} C_{f,h}(u)(-1)^{\langle u,y\rangle}\Big)^2$$

$$= \sum_{y\in\mathbb{F}_2^n} W_f^2(y)W_h^2(y)$$

$$\leq \Big(\sum_{y\in\mathbb{F}_2^n} W_f^2(y)\Big)\Big(\sum_{y\in\mathbb{F}_2^n} W_h^2(y)\Big)$$

$$= 2^{2n}\times 2^{2n}$$

$$= 2^{4n}.$$

Hence the result follows. □

The above preposition is the new way of generalizing the bounds as in Theorem 2 [17].

Proposition 3.5. *Suppose $f,g \in \mathcal{B}_{n,2}$, then*

$$\sum_{u\in\mathbb{F}_2^n} W_f^2(u)W_g^2(u)$$

$$\leq 2^{4n-1} + 2^{n-1}\Big((1-\mathcal{TO}(f,g))2^n(2^n-1)\Big)^2.$$

Proof. From Lemma 2 [18] we have

$$2^n\sum_{u\in\mathbb{F}_2^n} C_{f,g}^2(u) = \sum_{u\in\mathbb{F}_2^n} W_f^2(u)W_g^2(u).$$

But $\sum_{u\in\mathbb{F}_2^n} C_{f,g}^2(u) \leq \Big((1-\mathcal{TO}(f,g))2^n(2^n-1)\Big)^2$.
Therefore we have

$$\sum_{u\in\mathbb{F}_2^n} W_f^2(u)W_g^2(u) \leq 2^n\Big((1-\mathcal{TO}(f,g))2^n(2^n-1)\Big)^2. \quad (3)$$

Also we know that

$$\sum_{u\in\mathbb{F}_2^n} W_f^2(u)W_g^2(u) \leq \Big(\sum_{u\in\mathbb{F}_2^n} W_f^2(u)\Big)\Big(\sum_{u\in\mathbb{F}_2^n} W_g^2(u)\Big). \quad (4)$$

From (3) and (4) we have

$$2\sum_{u\in\mathbb{F}_2^n} W_f^2(u)W_g^2(u) \leq \Big((1-\mathcal{TO}(f,g))2^n(2^n-1)\Big)^2 + 2^n\Big(\sum_{u\in\mathbb{F}_2^n} W_f^2(u)\Big)\Big(\sum_{u\in\mathbb{F}_2^n} W_g^2(u)\Big)$$

$$\Rightarrow \sum_{u\in\mathbb{F}_2^n} W_f^2(u)W_g^2(u)$$

$$\leq 2^{4n-1} + 2^{n-1}\Big((1-\mathcal{TO}(f,g))2^n(2^n-1)\Big)^2.$$

Hence the result follows.
For $f=g$, we get

$$\sum_{u\in\mathbb{F}_2^n} W_f^4(u) \leq 2^{4n-1} + 2^{n-1}\Big((1-\mathcal{TO}(f))2^n(2^n-1)\Big)^2.$$

□

In the below given theorem we find the transparency order of a function fulfilling the propagation criterion about a linear subspace.

Theorem 3.6. *Suppose $f \in \mathcal{B}_{n,2}$ and let H be any subspace of $\mathbb{F}_2^n$, then for any $v \in \mathbb{F}_2^n$*

$$\mathcal{TO}(f) \leq 1-\frac{W_f^2(v) - \big(\mid H \mid \sum_{u\in H^\perp} C_f(u)\big)^{\frac{1}{2}}}{2^n(2^n-1)},$$

where $H^\perp$ denotes the dual of H, i.e., $H^\perp = \{p \in \mathbb{F}_2^n : \langle p,q\rangle = 0 \ \forall \ q \in H\}$.

Proof. Let H be a subspace of $\mathbb{F}_2^n$ and f be a Boolean function fulfilling the propagation criterion with respect to any nonzero element of H with co-dimension 1 or 2, then we have [1]

$$\sum_{w\in\mathbb{F}_2^n} W_f^2(w) = \mid H \mid \sum_{u\in E^\perp} C_f(u)$$

Using Corollary 5.1 [11] and (2), we have

$$2^{2n} = \mid H \mid \sum_{u\in H^\perp} C_f(u)$$

$$[W_f^2(v) - ((1 - \mathcal{TO}(f)2^n(2^n - 1))]^2 \leq \mid H \mid \sum_{u \in H^\perp} C_f(u)$$

Upon computation from above, we get

$$\mathcal{TO}(f) \leq 1 - \frac{W_f^2(v) - \big(\mid H \mid \sum\limits_{u \in H^\perp} C_f(u)\big)^{\frac{1}{2}}}{2^n(2^n - 1)}.$$

Hence the result is proved. □

4 Conclusions

In this paper Cross-Correlation and new interpretation of bent functions have been discussed in terms of transparency order of Boolean functions. The transparency order of Boolean functions by vector concatenation is discussed. The concept of complementary transparency order is introduced and some results of complementary transparency order with other cryptographic properties are evaluated. The transparency order of $(n-2)-$variable decomposition type bent functions is evaluated. The bounds on sum-of-squares of auto-correlation in terms of transparency order are generalized. Also transparency order of functions satisfying the propagation criterion is evaluated. Future scope of the work is to construct some more classes of Booleans functions which have better transparency order.There are numerous problems which need to be discussed like, how to construct low transparency order Boolean functions having higher nonlinearity ? How to correlate the work on nonlinearity and transparency order with cryptanalysis ? How to correlate this work in a q-ary setup and find its applications ?

Acknowledgements

The authors are thankful to the anonymous experienced referees for their valuable comments and suggestions which considerably enhance the originality of the paper.

REFERENCES

[1] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine. Propagation characteristics and Correlation-Immunity of highly nonlinear Boolean functions, In Advances in Cryptology - Eurocrypt 2000, Number 1807 in Lecture Notes in Computer Science, Springer-Verlag, Berlin, pp. 507–522, 2000.

[2] A. Jain, N.S. Chaudhari. Evolving Highly Nonlinear Balanced Boolean Functions with Improved Resistance to DPA Attacks, NSS 2015, LNCS 9408, Springer, Berlin, pp. 316–330, 2015.

[3] C. Carlet. On Highly Nonlinear S-Boxes and Their Inability to Thwart DPA Attacks, Progress in Cryptology-INDOCRYPT, LNCS 3797, Springer, Berlin, pp. 49–62, 2005.

[4] C. Carlet, D.K. Dalai, K.C. Gupta, S. Maitra. Algebraic immunity for cryptographically significant Boolean functions: analysis and construction, IEEE Trans. Inf. Theory, Vol. 52(7), pp. 3105–3121, 2006.

[5] E. Pasalic, S. Maitra, T. Johansson and P. Sarkar. New constructions of resilent and correlation immune Boolean functions achieving upper bounds on nonlinearity, In Proceedings of the Workshop on Cryptography and Coding Theory, Paris, 2001. Electronic Notes in Discrete Mathematics, Elsevier, Amsterdam, Vol. 6, 2000.

[6] E. Prouff. DPA Attacks and S-Boxes, FSE 2005, LNCS 3557, Springer, Berlin, pp. 424–441, 2005.

[7] K. Chakraborty, S. Sarkar, S. Maitra, B. Mazumdar, D. Mukhopadhyay, E. Prouff, Redefining the transparency order. Des. Codes Cryptogr. Vol. 82, pp. 95–115, 2017.

[8] L. E. Dickson. History of the Theory of Numbers, Chelsea, New York, Vol. II, 1919.

[9] P. Kocher, J. Jaffe, B. Jun. Differential Power Analysis, Advances in Cryptology–CRYPTO'99, LNCS 1666, Springer, Berlin, pp. 388–397, 1999.

[10] P. Kocher. Timing attacks on implementations of Diffie–Hellman,RSA, DSS, and other systems, Advances in Cryptology–CRYPTO'96, LNCS 1109, Springer, Berlin , pp. 104–113, 1996.

[11] P. Sarkar and S. Maitra. Cross-correlation analysis of cryptographically useful Boolean functions, Theory of Computing Systems, Vol. 35, pp.39-57, 2002.

[12] Q. Wang, P. Stanica, Transparency Order for Boolean functions: analysis and construction, Des. Codes Cryptogr., Vol. 87(9), pp. 2043-2059, 2019.

[13] S. Guilley, R. Pacalet. Differential Power Analysis Model and Some Results, CARDIS, pp. 127–142, 2004.

[14] S. Mangard, E. Oswald, T. Popp. Power Analysis Attacks-Revealing the Secrets of Smart Cards. Springer, Berlin, 2007.

[15] S. Picek, L. Batina, D. Jakobovic. Evolving DPA-Resistant Boolean Functions, PPSN 2014, LNCS 8672, Springer, Berlin pp. 812–821, 2014.

[16] W. Fischer, B.M. Gammel, O. Kniffler, J. Velten. Differential PowerAnalysis of Stream Ciphers, CT-RSA 2007, LNCS 4377, Springer, Berlin, pp. 257–270, 2006.

[17] X.M. Zhang and Y. Zheng. GAC—the criterion for global avalanche characteristics of cryptographic functions, Journal for Universal Computer Science, Vol. 1(5), pp. 316–333, 1995.

[18] Y. Zhou, M. Xie, and G. Xiao. On the GAC between two Boolean functions and the higher order nonlinearity, Inf. Sci., Vol. 180, pp. 256–265, 2010.

[19] Y. Zhou, Y. Wei, and F. Zhang. Measuring the Sum-of-Squares Indicator of Boolean Functions in Encryption Algorithm for Internet of Things, Hindawi Security and Communication Networks, 2019.