Research Article

On the Modified Transparency Order of \((n, m)\)-Functions

Yu Zhou\(^1\), Yongzhuang Wei\(^2\), Hailong Zhang\(^{3, 4}\) and Wenzheng Zhang\(^1\)

\(^1\)Science and Technology on Communication Security Laboratory, Chengdu 610041, China
\(^2\)Department of Communication and Information Engineering, Guilin University of Electronic Technology, Guilin 541004, China
\(^3\)State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
\(^4\)State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China

Correspondence should be addressed to Yu Zhou; zhouyu.zhy@tom.com

Received 15 December 2020; Accepted 8 July 2021; Published 3 August 2021

The concept of transparency order is introduced to measure the resistance of \((n, m)\)-functions against multi-bit differential power analysis in the Hamming weight model, including the original transparency order (denoted by \(TO\)), redefined transparency order (denoted by \(RTO\)), and modified transparency order (denoted by \(MTO\)). In this paper, we firstly give a relationship between \(MTO\) and \(RTO\) and show that \(RTO\) is less than or equal to \(MTO\) for any \((n, m)\)-functions. We also give a tight upper bound and a tight lower bound on \(MTO\) for balanced \((n, m)\)-functions. Secondly, some relationships between \(MTO\) and the maximal absolute value of the Walsh transform (or the sum-of-squares indicator, algebraic immunity, and the nonlinearity of its coordinates) for \((n, m)\)-functions are obtained, respectively. Finally, we give \(MTO\) and \(RTO\) for \((4, 4)\) S-boxes which are commonly used in the design of lightweight block ciphers, respectively.

1. Introduction

Differential power analysis (DPA) was introduced by Kocher et al. in [1] and is a well-known and thoroughly studied threat for implementations of block ciphers, like DES and AES [2].

Beierle et al. [3] validated the correlation power analysis attack through the Hamming distance power model. Fischer et al. [4] presented efficient differential power analysis of Gain and Trivium through carefully chosen IVs to eliminate the algorithmic noise. In 2005, Prouff [5] gave the model of the DPA resilience of the S-boxes and proposed the definition of the transparency order (denoted by \(T\theta\)) based on the autocorrelation coefficients for \((n, m)\)-functions. He obtained that S-boxes with smaller \(T\theta\) have higher DPA resilience and deduced the tightness of the upper bound and the lower bound on the \(T\theta\). In the same year, Carlet [6] obtained the lower bound on the transparency order and gave the relationship between the transparency order and the nonlinearity for Boolean functions. Next, Fan et al. [7] gave a fast method for calculating the transparency order by optimization cycle of the original algorithm.

In 2012, Fei et al. [8] proposed the confusion coefficient and obtained some relations between the success rate and the cryptographic algorithm. For power analysis attacks, the side-channel characteristic of the physical implementation can be seen as the signal-to-noise ratio (denote by \(SNR\)) [9]. Experimental results of DPA on both DES or AES verified this model with high accuracy and demonstrated effectiveness of the algorithmic confusion analysis and \(SNR\) extraction. Experimental results shown that the algorithm has better anti-noise performance than the original algorithm for present.

Chakraborty et al. [10] found the limitations of the definition in [5] and gave a redefined transparency order (denoted by \(RTO\)) based on the cross-correlation coefficients for \((n, m)\)-functions. Then, they were able to theoretically capture DPA in the Hamming weight model for hardware implementation with precharge logic. Picek et al.
[11] proposed a technique for constructions using the modified transparency order as a guiding metric. Wang and Stänică [12] obtained an upper bound on the redefined transparency order in terms of nonlinearity for Boolean functions and constructed two infinite class of balanced semibent Boolean functions with provably good transparency order.

But in 2020, Li et al. [13] put up a flaw in original transparency order [10] and gave the modified transparency order denoted by $\mathcal{MTO}$, obtained a lower bound on $\mathcal{MTO}$ based on the Walsh transform, and deduced the distribution of $\mathcal{MTO}$ values for sixteen optimal affine equivalent classes of (4,4) S-boxes.

So far, little attempt has been made to study the relationship between $\mathcal{RTO}$ and $\mathcal{MTO}$, and Li et al. [13] gave a lower bound on $\mathcal{MTO}$ for any $(n,m)$-functions based on Walsh spectrum, but not based on $m$. Moreover, how to further investigate the in-depth relationships between $\mathcal{RTO}$ and $\mathcal{MTO}$ with other cryptography indicators still appears to be an important issue.

In this article, we focus on some unresolved problems related to both $\mathcal{RTO}$ and $\mathcal{MTO}$. Firstly, we give the relationship between $\mathcal{MTO}$ and $\mathcal{RTO}$, and this result implies that $\mathcal{MTO}(F) \geq \mathcal{RTO}(F)$ for any $(n,m)$-functions $F$. We also obtain the upper bound and the lower bound on $\mathcal{MTO}$.

To design good S-boxes with respect to the $\mathcal{MTO}$ [13], we deduce some important connections between $\mathcal{MTO}$ and other cryptographic properties such as the sum-of-squares indicator, nonlinearity, the maximum absolute of Walsh transform, and algebraic immunity of the coordinate functions of S-boxes. In particular, it is shown that these results have a direct influence on the resistance to DPA attacks. More precisely, the smaller the sum-of-squares indicator (or the maximum absolute of Walsh transform) of the coordinate functions of a given $(n,m)$-function, the larger the $\mathcal{MTO}$, whereas a higher nonlinearity (or algebraic immunity) of the coordinate functions of a given $(n,m)$-function also implies a larger $\mathcal{MTO}$ (not desirable). Furthermore, there is also a connection between the algebraic immunity and transparency order which essentially indicates (along with other trade-offs) that the design of cryptographically secure S-boxes is hardly achievable if the protection against DPA attacks is taken into account.

Finally, we give the $\mathcal{MTO}$ and $\mathcal{RTO}$ for (4,4) S-boxes which are commonly used in some lightweight block ciphers, it implies that $\mathcal{MTO}$ is better than $\mathcal{RTO}$ from the perspective of information leakage.

This paper is organized as follows. In Section 2, we introduce the basic concepts and notions. In Section 3, the tightness of the upper bound and the lower bound on the modified transparency order of $(n,m)$-functions is derived. In Section 4, some relationships between $\mathcal{MTO}(F)$ and other cryptographic properties are derived. Section 5 gives some data analysis results for some (4,4) S-boxes. Section 6 concludes this paper.

## 2. Preliminaries

Let $\mathbb{B}_n$ be the set of $n$-variable Boolean functions. We denote by $\oplus$ the addition modulo two performed in $\mathbb{F}_2$ and the vector space $\mathbb{F}_2^n$. The support of a Boolean function $f \in \mathbb{B}_n$ is defined as $\text{supp}(f) = \{(x_1, \ldots, x_n) \in \mathbb{F}_2^n | f(x_1, \ldots, x_n) = 1\}$. The Hamming weight of $f$ is denoted by $\text{wt}(f)$ and corresponds to the cardinality of its support $\text{wt}(f) = |\text{supp}(f)|$. A Boolean function $f$ is said to be balanced if its truth table contains equal number of ones and zeros, i.e., $\text{wt}(f) = 2^{n-1}$. The set of affine functions, whose algebraic degree $\deg (f) \leq 1$ is denoted by $\mathcal{A}_n$. Especially, an affine function with the constant term equal to zero is called a linear function.

In this paper, let $0^n = \left\{0, \ldots, 0\right\}_{n}$ be the zero vector in $\mathbb{F}_2^n$.

### Definition 1.
Let $f \in \mathbb{B}_n$. The Walsh spectrum of $f$ is defined by

$$\mathcal{F}(f \oplus \varphi_\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \varphi_\alpha(x)}, \quad \alpha \in \mathbb{F}_2^n,$$

where $\varphi_\alpha(x) = \alpha \cdot x = \alpha_1 x_1 \oplus \cdots \oplus \alpha_n x_n$, $x = (x_1, x_2, \ldots, x_n)$, $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. The nonlinearity of $f$ can be computed using

$$N_f = 2^{n-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}_2^n} |\mathcal{F}(f \oplus \varphi_\alpha)|.$$

Let $f, g \in \mathbb{B}_n$. The cross-correlation function between $f$ and $g$ is defined by

$$\Delta_{f,g}(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus g(x) \oplus \alpha}, \quad \alpha \in \mathbb{F}_2^n.$$

In particular, when $f = g$, then the autocorrelation function of $f \in \mathbb{B}_n$ is given by

$$\Delta_f(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x) \oplus \alpha}, \quad \alpha \in \mathbb{F}_2^n.$$

For more research on the autocorrelation function and the cross-correlation function of Boolean functions, refer to reference [14].

Two functions $f, g \in \mathbb{B}_n$ are said to be perfectly uncorrelated if $\Delta_{f,g}(\alpha) = 0$, for any $\alpha \in \mathbb{F}_2^n$. From [15], if $f$ and $g$ are perfectly uncorrelated, then $\mathcal{F}(f \oplus \varphi_\alpha) \mathcal{F}(g \oplus \varphi_\alpha) = 0$ for any $\alpha \in \mathbb{F}_2^n$.

### Definition 2 (see [16]).
The two indicators capturing the global avalanche characteristics (GACs) of a Boolean function $f \in \mathbb{B}_n$ are given by

$$\sigma_f = \sum_{a \in \mathbb{F}_2^n} |\Delta_f(\alpha)|^2,$$

$$\Delta_f = \max_{a \in \mathbb{F}_2^n \cup \mathbb{F}_2^{n+1}} |\Delta_f(\alpha)|.$$
In 2010, Zhou et al. [17] generalized GAC and gave the global avalanche characteristics between two Boolean functions \( f, g \in \mathbb{B}_n \):

\[
\sigma_{f,g} = \sum_{a \in \mathbb{F}_2^n} \left| \Delta_{f,g}(a) \right|^2, \quad \Delta_{f,g} = \max_{a \in \mathbb{F}_2^n} \left| \Delta_{f,g}(a) \right|. \tag{6}
\]

For two positive integers \( n \) and \( m \), a function \( F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n \) is called an \((n, m)\)-function. Such a function \( F \) can be viewed as a collection of its coordinate Boolean functions, and thus \( F = (f_1, \ldots, f_m) \), where \( f_i : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \). An \((n, m)\)-function \( F \) is balanced if and only if its component functions are balanced, meaning that for every \( \nu \in \mathbb{F}_2^n \), the Boolean function \( \nu \cdot F \) is balanced. The original transparency order \([5]\) and the redefining transparency order \([10]\) are for balanced \((n, m)\) functions. In this paper, in order to expand the research scope of \((n, m)\)-function, we extend the balanced \((n, m)\)-function to any \((n, m)\)-function, which makes our results more universal (see Definition 3 and Definition 4).

**Definition 3** (see [10]). Let \( F = (f_1, \ldots, f_m) \) be an \((n, m)\)-function. The redefined transparency order of \( F \), based on the cross-correlation properties of \( F \), is defined by

\[
\mathcal{RTOP}(F) = \max_{\beta \in \mathbb{F}_2^n} \left\{ m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^n} \left| \sum_{j=1}^m (-1)^{\beta_j} \Delta_{f_j}(a) \right|^2 \right\}, \tag{7}
\]

where \( \beta = (\beta_1, \beta_2, \ldots, \beta_m), \beta_j \in \mathbb{F}_2 \).

In 2019, Li et al. gave the modified transparency order in [13].

**Definition 4** (see [13]). Let \( F = (f_1, \ldots, f_m) \) be an \((n, m)\)-function. The modified transparency order of \( F \), based on the cross-correlation properties of \( F \), is defined by

\[
\mathcal{MTOP}(F) = \max_{\beta \in \mathbb{F}_2^n} \left\{ m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^n} \left| \sum_{j=1}^m (-1)^{\beta_j} \Delta_{f_j}(a) \right|^2 \right\}. \tag{8}
\]

Note that

\[
(-1)^{\beta_j} \Delta_{f_j}(a) = \Delta_{f_{\beta_j}, f_{\beta_j}}(a), \tag{9}
\]

and for research convenience, let

\[
\Gamma_{\beta} = m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^n} \left| \sum_{j=1}^m \Delta_{f_{\beta_j}, f_{\beta_j}}(a) \right|. \tag{10}
\]

Thus,

\[
\mathcal{MTOP}(F) = \max_{\beta \in \mathbb{F}_2^n} \Gamma_{\beta}. \tag{11}
\]

### 3. Bounds on the Modified Transparency Order

Based on Definition 4, a lower bound on \( \mathcal{MTOP} \) was derived in [13] in terms of the Walsh spectrum of the coordinate functions of \( F \), but this lower bound is very complex. In order to obtain a tight lower and upper bounds on \( \mathcal{MTOP} \), we firstly give a relationship between \( \mathcal{MTOP} \) and \( \mathcal{RTOP} \).

**Lemma 1** (see [17]). Let \( f, g \in \mathbb{B}_n \). Then,

\[
\sum_{a \in \mathbb{F}_2^n} \Delta_{f,g}(a) = (2^n - 2\text{wt}(f))(2^n - 2\text{wt}(g)). \tag{12}
\]

**Theorem 1.** Let \( F = (f_1, \ldots, f_m) \) be an \((n, m)\)-function. Then,

\[
\mathcal{MTOP}(F) \leq \mathcal{RTOP}(F). \tag{13}
\]

**Proof.** By using the inequality \( \sum_{i=1}^m a_i \leq \sum_{i=1}^m |a_i| \) for any \( a_i \in \mathbb{R} \), we have

\[
\sum_{j=1}^m \sum_{i=1}^m (-1)^{\beta_i} \Delta_{f,j}(a) \leq \sum_{j=1}^m \sum_{i=1}^m (-1)^{\beta_i} \Delta_{f,j}(a), \tag{14}
\]

For any \( a \in \mathbb{F}_2^n \), we have

\[
m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^n} \left| \sum_{j=1}^m (-1)^{\beta_j} \Delta_{f,j}(a) \right|^2 \geq m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^n} \left| \sum_{j=1}^m (-1)^{\beta_j} \Delta_{f,j}(a) \right|^2 \tag{15}
\]

Based on the above equation, we have \( \mathcal{MTOP}(F) \geq \mathcal{RTOP}(F) \).

**Remark 1.** From the proof process, we can know that \( \mathcal{MTOP}(F) \geq \mathcal{RTOP}(F) \) for any \((n, m)\)-function \( F \), including balanced functions and unbalanced functions.

Although at present we cannot theoretically give the condition on \( \mathcal{RTOP}(F) = \mathcal{MTOP}(F) \) of \((n, m)\)-functions \( F = (f_1, f_2, \ldots, f_m) \), we can give an example with \( \mathcal{RTOP}(F) = \mathcal{MTOP}(F) \) (see Example 1).

In the following, we give a tight upper bound and a tight lower bound on \( \mathcal{MTOP}(F) \) by using the perfectly uncorrelated functions.

**Theorem 2.** Let \( F = (f_1, \ldots, f_m) \) be a balanced \((n, m)\)-function. If the coordinate functions \( f_i \) and \( f_j \) are perfectly uncorrelated for \( 1 \leq i \neq j \leq m \), then

\[
0 \leq \mathcal{MTOP}(F) \leq m. \tag{16}
\]

**Proof.** On the one hand, from Definition 4 and Lemma 1, we have
\[ \Gamma_F^\beta = m - \frac{1}{2^n - 2} \sum_{a \in \mathbb{F}_2^n} \sum_{j=1}^{m} \sum_{i=1}^{m} \Delta_{f, \phi_i, f, \phi_j} (a) \]

\[ = m - \frac{1}{2^n - 2} \sum_{a \in \mathbb{F}_2^n} \sum_{j=1}^{m} \Delta_{f, \phi_i, f, \phi_j} (a) + \cdots + \Delta_{f, \phi_i, f, \phi_j} (a) \]

\[ \leq m - \frac{1}{2^n - 2} \sum_{a \in \mathbb{F}_2^n} \sum_{j=1}^{m} \Delta_{f, \phi_i, f, \phi_j} (a) + \cdots + \Delta_{f, \phi_i, f, \phi_j} (a) \]

\[ = m - \frac{1}{2^n - 2} \sum_{a \in \mathbb{F}_2^n} \sum_{j=1}^{m} \left[ \Delta_{f, \phi_i, f, \phi_j} (a) + \cdots + \Delta_{f, \phi_i, f, \phi_j} (a) \right] \]

\[ = m - \frac{1}{2^n - 2} \sum_{j=1}^{m} \left[ \Delta_{f, \phi_i, f, \phi_j} (a) + \cdots + \Delta_{f, \phi_i, f, \phi_j} (a) \right] \]

\[ = m - \frac{1}{2^n - 2} \sum_{j=1}^{m} \left[ \Delta_{f, \phi_i, f, \phi_j} (a) + \cdots + \Delta_{f, \phi_i, f, \phi_j} (a) \right] \]

\[ = m - \frac{1}{2^n - 2} \sum_{j=1}^{m} \left[ \Delta_{f, \phi_i, f, \phi_j} (a) + \cdots + \Delta_{f, \phi_i, f, \phi_j} (a) \right] \]

(17)

Since \( F = (f_1, \ldots, f_m) \) is a balanced \((n, m)\)-function, then \( f_k (1 \leq k \leq m) \) and \( f_i \oplus f_j (1 \leq i < j \leq m) \) are balanced functions. That is, \( \text{wt}(f_k) = \text{wt}(f_i \oplus f_j) = 2^{n-1} \) for any \( 1 \leq k \leq m \) and \( 1 \leq i < j \leq m \). We have \( \Delta_{f, f_i, f_j} (0^n) = 2^n - 2\text{wt}(f_i \oplus f_j) = 0 \) and \( 2^n - 2\text{wt}(f_k) = 0 \) for any \( 1 \leq i < j \leq m, 1 \leq k \leq m \).

Thus, \( \Gamma_F^\beta \leq m \), that is, \( \mathcal{F} \mathcal{C}(F) \leq m \).

On the other hand, if the coordinate functions \( f_i \) and \( f_j \) are perfectly uncorrelated for \( 1 \leq i \neq j \leq m \), then \( \Delta_{f_i, f_j} (a) = 0 \) for any \( a \in \mathbb{F}_2^n \) and \( 1 \leq i \neq j \leq m \).

From Definition 4, we have

\[ \Gamma_F^\beta = m - \frac{1}{2^n - 2} \sum_{a \in \mathbb{F}_2^n} \sum_{j=1}^{m} \sum_{i=1}^{m} \Delta_{f, \phi_i, f, \phi_j} (a) \]

\[ = m - \frac{1}{2^n - 2} \sum_{a \in \mathbb{F}_2^n} \sum_{j=1}^{m} \Delta_{f_i, a}(a) + \cdots + \Delta_{f_m, a}(a) \]

\[ \geq m - \frac{1}{2^n - 2} \sum_{a \in \mathbb{F}_2^n} \left[ \sum_{j=1}^{m} \left| \Delta_{f_i, a}(a) \right| + \sum_{j=1}^{m} \left| \Delta_{f_j, a}(a) \right| + \cdots + \sum_{j=1}^{m} \left| \Delta_{f_m, a}(a) \right| \right] \]

(18)

By Cauchy's inequality and \( 2^n \leq \sigma_{f_j} = \sum_{a \in \mathbb{F}_2^n} \left| \Delta_{f_j, a}(a) \right|^2 \leq 2^{2n} \) for any \( 1 \leq i \leq m \) in [16], we have

\[ 2^{m} - 2^n \geq \sigma_{f_j} - \Delta_{f_j, a}(0^n) = \sum_{a \in \mathbb{F}_2^n} \left| \Delta_{f_j, a}(a) \right|^2 \]

\[ \geq \left( \sum_{a \in \mathbb{F}_2^n} \left| \Delta_{f_j, a}(a) \right| \right)^2 \]

\[ \geq \frac{\left( \sum_{a \in \mathbb{F}_2^n} \left| \Delta_{f_j, a}(a) \right| \right)^2}{2^n - 1} \]

(19)

Thus,

\[ \sum_{a \in \mathbb{F}_2^n} \left| \Delta_{f_j, a}(a) \right| \leq 2^n \left( 2^n - 1 \right), \quad 1 \leq i \leq m. \]  

(20)

From equation (20), we have

\[ \Gamma_F^\beta \geq m - \frac{m \cdot 2^n (2^n - 1)}{2^{2n} - 2^n} = 0. \]

That is, \( \mathcal{F} \mathcal{C}(F) \geq 0 \).

In the following, we give two examples for reaching the upper and lower bounds on \( \mathcal{F} \mathcal{C}, \) respectively.

**Example 1.** Let \( F = (f_1, f_2) \) be an \((n, m)\)-function \((m = 2)\) and \( f \) be a bent function. Its coordinate functions are specified as

\[ f_1 (x) = f (x), f_2 (x) = f (x) \oplus 1. \]

Then, \( f_1 \) and \( f_2 \) are bent functions. We know \( \Delta_{f, f_1} (a) = 0 \) and \( \Delta_{f, f_2} (a) = 0 \) for any \( a \in \mathbb{F}_2^n \) and \( 1 \leq i \neq j \leq m \). We have

\[ \Gamma_F^\beta = m - \frac{1}{2^n - 2} \sum_{a \in \mathbb{F}_2^n} \sum_{j=1}^{m} \sum_{i=1}^{m} \Delta_{f, \phi_i, f, \phi_j} (a) \]

\[ = m - \frac{1}{2^n - 2} \sum_{a \in \mathbb{F}_2^n} \sum_{j=1}^{m} \sum_{i=1}^{m} \Delta_{f, \phi_i, f, \phi_j} (a) \]

\[ = m

(23)

and thus \( \mathcal{F} \mathcal{C}(F) = m = 2 \). We also obtain \( \mathcal{R} \mathcal{C}(F) = m = 2 \).

**Example 2.** Let \( F = (f_1, f_2) \) be a \((4, 2)\)-function. Its coordinate functions are specified as

\[ f_1 (x) = x_1 \oplus x_2, \]

\[ f_2 (x) = x_3 \oplus x_4. \]

Then, \( F \) is balanced \((n = 4, m = 2)\). We know \( \Delta_{f, f_1} (a) = 2^n \) and \( \Delta_{f, f_2} (a) = 0 \) for any \( a \in \mathbb{F}_2^n \) and \( 1 \leq i \neq j \leq m \). Then, we have
\[
\Gamma^\beta_F = m - \frac{1}{2^{2n} - 2^n} \sum_{\alpha \in \mathbb{F}_2^n} \left| \sum_{i=1}^m \sum_{j=1}^m \Delta_{f,\beta_i, f, \beta_j}(a) \right|
\]
\[
= m - \frac{m2^n (2^{2n}-1)}{2^{2n} - 2^n} \quad (25)
\]
and thus \(\mathcal{MTF}(F) = 0\).

In particular, we give the modified transparency order for any \((n,1)\)-function.

**Corollary 1.** Let \(f \in \mathbb{B}_n\). Then,
\[
0 \leq \mathcal{MTF}(f) \leq 1. \quad (26)
\]

**Proof.** If \(m = 1\) in Definition 4, then
\[
\mathcal{MTF}(f) = 1 - \frac{1}{2^{2n} - 2^n} \sum_{\alpha \in \mathbb{F}_2^n} \left| \Delta_f(a) \right|. \quad (27)
\]
Note that \(0 \leq |\Delta_f(a)| \leq 2^n\) for any \(a \in \mathbb{F}_2^n\). Then, \(0 \leq \mathcal{MTF}(f) \leq 1\). \(\mathcal{MTF}(f) = 0\) if and only if \(|\Delta_f(a)| = 2^n\) for any \(a \in \mathbb{F}_2^n\), that is, \(f\) is an affine function. \(\mathcal{MTF}(f) = 1\) if and only if \(|\Delta_f(a)| = 0\) for any \(a \in \mathbb{F}_2^n\), that is, \(f\) is a bent function. □

**Remark 2.** Corollary 1 is a special case of Theorem 2. It also shows that both the upper bound and the lower bound on \(\mathcal{MTF}\) can be reached.

### 4. The Relationships between \(\mathcal{MTF}\) and Some Cryptographic Properties

In this section, we use the sum-of-squares indicator to establish some links between \(\mathcal{MTF}\) and some cryptographic indicators. These links can help us understand \(\mathcal{MTF}\) more deeply and lay a foundation for designing and analyzing S-boxes. In the following, we give a relationship between \(\mathcal{MTF}\) and the sum-of-squares indicator, and this result is the basis of Corollaries 3 and 4.

#### 4.1. The Relationships between \(\mathcal{MTF}\) and the Sum-of-Squares Indicator

**Theorem 3.** Let \(F = (f_1, \ldots, f_m)\) be a balanced \((n,m)\)-function. Then,
\[
\mathcal{MTF}(F) \geq m - \frac{1}{2^{2n} - 2^n} \sum_{\alpha \in \mathbb{F}_2^n} \left| \sum_{i=1}^m \sum_{j=1}^m \Delta_{f,\beta_i, f, \beta_j}(a) \right| \geq m - \frac{1}{2^{2n} - 2^n} \left( (2^n-1)m^2 \sum_{j=1}^m \sigma_{f,f_j} \right)^{1/2} \geq m - \frac{1}{2^{2n} - 2^n} \left( \frac{\sqrt{\sum_{j=1}^m \sigma_{f,f_j}^2}}{2^n \sqrt{2^n-1}} \right)^{1/2} \geq m - \frac{1}{2^{2n} - 2^n} \left( \frac{\sqrt{\sum_{j=1}^m \sigma_{f,f_j}^2}}{2^n \sqrt{2^n-1}} \right)^{1/2} \geq m \left( 1 - \frac{1}{2^{2n} - 2^n} \right) \left( \frac{\sqrt{\sum_{j=1}^m \sigma_{f,f_j}^2}}{2^n \sqrt{2^n-1}} \right)^{1/2}
\]

Because \(\sigma_{f,g} \leq \sqrt{\sigma_f \sigma_g}\) for any \(f, g \in \mathbb{B}_n\) [18], we have
\[
\Gamma^\beta_F \geq m \left( 1 - \frac{\sqrt{\sum_{j=1}^m \sigma_{f,f_j}^2}}{2^n \sqrt{2^n-1}} \right)^{1/2} \geq m \left( 1 - \frac{\sum_{j=1}^m \sigma_{f,f_j}}{2^n \sqrt{2^n-1}} \right).
\]

**Proof.** By using the Cauchy–Schwarz inequality and for any \(\beta = (\beta_1, \beta_2, \ldots, \beta_m) \in \mathbb{F}_2^m\), we have
\[
\sum_{i=1}^m \left| \sum_{j=1}^m \Delta_{f,\beta_i, f, \beta_j}(a) \right|^2 \leq m \sum_{j=1}^m \left| \sum_{i=1}^m \Delta_{f,\beta_i, f, \beta_j}(a) \right|^2 \leq m^2 \sum_{j=1}^m \Delta_{f,\beta_i, f, \beta_j}(a)^2.
\]
\[
\sum_{\alpha \in \mathbb{F}_2^n} \left| \sum_{i=1}^m \sum_{j=1}^m \Delta_{f,\beta_i, f, \beta_j}(a) \right|^2 \leq m \sum_{j=1}^m \left| \sum_{i=1}^m \Delta_{f,\beta_i, f, \beta_j}(a) \right|^2 \leq m^2 \sum_{j=1}^m \Delta_{f,\beta_i, f, \beta_j}(a)^2.
\]

Since \(F\) is a balanced \((n,m)\)-function, \(f, \sigma f, f_j\) is balanced for \(1 \leq i < j \leq m\), that is, \(\Delta_{f,\beta_i, f, \beta_j}(0^n) = 0\). Thus,
\[
\sum_{\alpha \in \mathbb{F}_2^n} \left| \sum_{i=1}^m \sum_{j=1}^m \Delta_{f,\beta_i, f, \beta_j}(a) \right|^2 \leq \left( 2^n - 1 \right) \sum_{\alpha \in \mathbb{F}_2^n} \left( \sum_{i=1}^m \sum_{j=1}^m \Delta_{f,\beta_i, f, \beta_j}(a) \right)^2 \leq \left( 2^n - 1 \right) m^2 \sum_{j=1}^m \sum_{i=1}^m \Delta_{f,\beta_i, f, \beta_j}(a)^2 \leq \left( 2^n - 1 \right) m^2 \sum_{j=1}^m \sum_{i=1}^m \Delta_{f,\beta_i, f, \beta_j}(a)^2.
\]

Therefore,
\[
\mathcal{MTF}(F) \geq \left( 1 - \frac{1}{2^{2n} - 2^n} \right) \left( \frac{\sqrt{\sum_{j=1}^m \sigma_{f,f_j}^2}}{2^n \sqrt{2^n-1}} \right)^{1/2} \geq \left( 1 - \frac{1}{2^{2n} - 2^n} \right) \left( \frac{\sum_{j=1}^m \sigma_{f,f_j}}{2^n \sqrt{2^n-1}} \right).
\]
From Definition 4, we know that
\[
\mathcal{MTO}(F) = \max_{\beta \in F_2} \beta \sigma_f.
\] (33)

Thus,
\[
\mathcal{MTO}(F) \geq 1_F^\beta \geq m \left[ 1 - \frac{\sum_{i=1}^{m} \sigma_f}{2^n} \right].
\] (34)

Remark 3. Theorem 3 gives one relationship between \( \mathcal{MTO}(F) \) and \( \sigma_f(1 \leq i \leq m) \), which implies that the smaller \( \sigma_f(1 \leq i \neq j \leq m) \), the bigger the \( \mathcal{MTO}(F) \).

Based on Theorem 3, we give some lower bounds on \( \mathcal{MTO} \) by nonlinearity and algebraic immunity.

**Corollary 2.** Let \( F = (f_1, \ldots, f_m) \) be a balanced \((n, m)\)-function. Then,
\[
\mathcal{MTO}(F) \geq m \left[ 1 - \frac{\sum_{i=1}^{m} \sigma_f}{2^n} \right].
\] (35)

Proof. Zheng and Zhang [19] obtained \( \sigma_f \leq 2^n[\mathcal{L}_f]^2 \) for any \( f \in \mathbb{B}_n \), where \( \mathcal{L}_f = \max_{w \in \mathbb{F}_2^n} \mathcal{F}(f \oplus \varphi_w) \) for any \( 1 \leq i \leq m \), and thus this result is easily proved. \( \Box \)

**Corollary 3.** Let \( F = (f_1, \ldots, f_m) \) be a balanced \((n, m)\)-function. Then,
\[
\mathcal{MTO}(F) \geq m \left[ 1 - \frac{\sum_{i=1}^{m} (2^n - 2N_{f_i})}{2^n (2^n - 1)} \right].
\] (36)

Proof. Since \( \mathcal{L}_{f_i} = 2^n - 2N_{f_i} \) for \( 1 \leq i \leq m \), this result is easily proved. \( \Box \)

**Corollary 4.** Let \( F = (f_1, \ldots, f_m) \) be a balanced \((n, m)\)-function. Then,
\[
\mathcal{MTO}(F) \geq m \left[ 1 - \frac{1}{\sqrt{2^n (2^n - 1)}} \right],
\] (37)

where \( A = \sum_{i=1}^{m} \left( 2^n - 4\sum_{k=0}^{\sigma_f-2} \left( \frac{n-1}{k} \right) \right), B = \sum_{j=1}^{m} \). \( \Box \)

Proof. Carlet [20] obtained \( N_{f_i} \geq 2\sum_{i=0}^{\sigma_f-2} \left( \frac{n-1}{i} \right) \) for \( 1 \leq i \leq m \), and thus this result is easily proved. \( \Box \)

**Remark 4.** From Corollaries 3 and 4, we have

1. The larger the \( N_{f_i} \) (or \( \sigma_f(1 \leq i \leq m) \)), the larger the \( \mathcal{MTO}(F) \).

2. For the conventional attacks, S-boxes should have higher nonlinearity, algebraic immunity, good the sum-of-squares indicators, etc. For the differential power analysis, S-boxes should have lower the transparency order. Therefore, the trade-off among these indicators should be considered when designing cryptographic algorithm components in practice.

### 4.2. The Relationships between \( \mathcal{MTO} \) and Hamming Weight

In this section, we give an upper bound on \( \mathcal{MTO} \) by the Hamming weight of coordinate functions.

**Theorem 4.** Let \( F = (f_1, \ldots, f_m) \) be an \((n, m)\)-function and \( \mathrm{wt}(f_i) = 2^{n-1} (1 \leq i \leq m) \). Then, for any \( \beta = (\beta_1, \beta_2, \ldots, \beta_m) \in \mathbb{F}_2^m \),
\[
\mathcal{MTO}(F) \leq m - \frac{\sum_{j=1}^{m} \sum_{i=1}^{m} (-1)^{\beta \beta_i} \mathrm{wt}(f_i \oplus f_j)}{2^{2n} - 2^n}.
\] (38)

Proof. Using the relation of absolute value inequality and Lemma 1, since \( f_i \) is a balanced function for \( 1 \leq i \leq m \), we have
\[ I_f^\beta = m - \frac{\sum_{\alpha \in F_m^2} \left| \sum_{j=1}^{m} \left| \sum_{i=1}^{m} \Delta f_{\alpha \beta_i, f_{\alpha \beta_j}}(a) \right| 2^{2n} - 2^n \right|}{2^{2n} - 2^n} \leq m - \frac{\sum_{\alpha \in F_m^2} \sum_{j=1}^{m} \Delta f_{\alpha \beta_i, f_{\alpha \beta_j}}(a)}{2^{2n} - 2^n} = m - \frac{\sum_{j=1}^{m} \sum_{i=1}^{m} \left[ \Delta f_{\alpha \beta_i, f_{\alpha \beta_j}}(a) - \Delta f_{\alpha \beta_i, f_{\alpha \beta_j}}(0^n) \right]}{2^{2n} - 2^n} = m - \frac{1}{2^{2n} - 2^n} \sum_{j=1}^{m} \sum_{i=1}^{m} \left[ (2^n - 2^{\text{wt}(f_{\alpha \beta_j})}) \left[ 2^n - 2^{\text{wt}(f_{\alpha \beta_j})} - \Delta f_{\alpha \beta_i, f_{\alpha \beta_j}}(0^n) \right] \right] = m - \frac{\sum_{j=1}^{m} \sum_{i=1}^{m} (-1)^{\delta_{\beta_i} \text{wt}(f_{\alpha \beta_j})}}{2^{2n} - 2^n}, \]

which proves the result. \( \square \)

**Remark 5.** If \( \text{wt}(f_{\alpha \beta_j}) = 2^{n-1} \) for any \( 1 \leq i \neq j \leq m \), then \( \mathcal{MTO} (F) \leq m - (m/2^n - 1) \). This implies that \( \mathcal{MTO} (F) \leq m - (m/2^n - 1) \) for balanced \((n,m)\)-functions \( F = (f_1, \ldots, f_m) \), \( f_i \in \mathbb{B}_n, 1 \leq i \leq m \).

**Corollary 5.** Let \( F = (f_1, \ldots, f_m) \) be a balanced \((n,m)\)-function. Then,

\[ 0 \leq \mathcal{MTO} (F) \leq m - \frac{m}{2^n - 1}. \quad (40) \]

Wang and Stănică [12] gave a tight upper bound on the transparency order in terms of nonlinearity for a Boolean function and obtained a lower bound between transparency order and nonlinearity for a Boolean function. In the following, for a Boolean function, we also give one upper bound and some lower bounds on \( \mathcal{MTO} \).

**Corollary 6.** Let \( f \in \mathbb{B}_n \). Then,

1. \( \mathcal{MTO} (f) \geq 1 - (\sqrt{2^n - 1}/\sqrt{2^n - 2^n}) \sqrt{2^n - 2^n} \)
2. \( \mathcal{MTO} (f) \geq 1 - (\sqrt{2^n - 2^n}/\sqrt{2^n - 2^n}) \sqrt{2^n - 2^n} \)
3. \( \mathcal{MTO} (f) \geq 1 - (\sqrt{2^n - MTO} \sqrt{2^n - 2^n}) \sqrt{2^n - 2^n} \)
4. \( \mathcal{MTO} (f) \leq 1 - (\sqrt{2^n - 2^{\text{wt}(f)})^2 - 2^n}/\sqrt{2^n - 2^n}) \sqrt{2^n - 2^n} \)

Remark 6. In this section, we have the following facts.

1. Theorem 3 and Corollaries 2–5 are all about balanced Boolean functions, but Corollary 6 is about Boolean function (including balanced and unbalanced Boolean functions).

2. Wang and Stănică [12] gave the upper bound on \( \mathcal{MTO} \) by the nonlinearity of Boolean function; here we give the lower bounds on \( \mathcal{MTO} \) by the nonlinearity, the sum-of-squares indicator, and the maximum absolute of Wash transform, respectively.

3. These results show that the smaller the sum-of-squares indicator (or the maximal absolute value of Walsh spectrum) of its coordinate, the bigger the modified transparency order, and the bigger the nonlinearity (or the algebraic immunity) of its coordinate, the bigger the modified transparency order.

**5. Data Analysis of \((4,4)\) S-Boxes**

In this section, we give \( \mathcal{MTO} \) or \( \mathcal{MTO} \) of three types of 4-bit S-boxes: (1) some lightweight S-boxes used in some well-known encryption algorithms, (2) 16 classes of optimal \((4,4)\) S-boxes, and (3) 302 affine equivalent \((4,4)\) S-boxes. Thus, we give the analysis results of S-boxes in three subsections.

5.1. \( \mathcal{MTO} \) and \( \mathcal{MTO} \) of Some Known S-Boxes in Well-Known Encryption Algorithms. We give the \( \mathcal{MTO} \) and \( \mathcal{MTO} \) of S-boxes in some well-known encryption algorithms (such as Pride [21], Midori [22], Gift [23], MANTIS [3], SKINNY [3], PRESENT [24], Prince [25], Marvin [26], Piccolo [27], and Lblock [28]) in Table 1.

The data in Table 1 show that \( \mathcal{MTO} \leq \mathcal{MTO} \) for a given S-box. This is consistent with Theorem 1.

5.2. The \( \mathcal{MTO} \) of 16 Optimal \((4,4)\) S-Boxes. In 2007, Leander et al. gave 16 different optimal balanced \((4,4)\) S-boxes based on affine equivalence in [29]. The representatives of the truth table are given in Table 2.
In the algorithm design, we want to know the exact optimal classes in [13]. But from these data, we cannot find many of MTO S-boxes (\( \circ A \)) (two 8-bit S-box and different affine transformations \( G \)). Especially, we get the detailed distribution of MTO of \( A \cdot G_0 \) and \( A \cdot G_3 \) in Tables 5 and 6, respectively. The calculation results of other \( G_i \) (\( i = 1, 2, 4, 5, \ldots, 15 \)) are similar to Table 5, which is ignored due to the limited length of this paper.

### 5.3. The RTO and MTO of 302 Affine Equivalent (4,4) S-Boxes.

There are 302 affine equivalence classes of 4-bit S-boxes [30]. We compute MTO and RTO of all 302 S-boxes of size 4 \( \times 4 \). Our simulations show that the modified transparency order is confined within the range 2.666667 \( \leq \text{RTO}(F) \leq 3.533333 \), but 0 \( \leq \text{RTO}(F) \leq 2.766667 \) in Table 7–9. We summarize the comparison of modified transparency order and the redefined transparency.
order in Tables 7–9 and find that $MTO \geq RTO$, and these data show that Hypothesis 1 is correct.

Remark 7. In Table 10, the number of affine equivalence classes whose modified transparency order lies in the range $MTO_{(4,4)} = [3.066667, 3.466667]$ is equal to $287 = 40 + 69 + 40 + 49 + 41 + 47$, which corresponds to about 95.03% of their total number. This simply means that for a randomly selected $(4,4)$ S-box, the probability that its transparency order is in the range $MTO_{(4,4)}$ is approximately 95.03%, which is quite high. This again questions the whole idea of embedding the protection against DPA attacks.
Table 6: Distribution of \( \text{MTO} \) of affine equivalent S-boxes of \( G_3 \).

| Class | \( \text{MTO} (A \circ G_3) \) | Number | Per (%) |
|-------|-----------------|--------|---------|
| 1     | 3.133333        | 7200   | 35.714286 |
| 2     | 3.200000        | 3960   | 19.642857 |
| 3     | 3.266667        | 1800   | 8.928571  |
| 4     | 3.333333        | 7200   | 35.714286 |

Table 7: Comparison of \( \text{RTO} \) and \( \text{MTO} \) of \((4, 4)\) S-boxes (III).

| \( \text{RTO} \) | Number | \( \text{MTO} \) | Number |
|-----------------|--------|-----------------|--------|
| 2.633333        | 9      | 3.066667        | 3      |
|                 |        | 3.133333        | 1      |
|                 |        | 3.200000        | 1      |
|                 |        | 2.666667        | 2      |
| 2.666667        | 7      | 2.933333        | 3      |
|                 |        | 3.066667        | 1      |
|                 |        | 2.200000        | 1      |
| 2.700000        | 1      | 3.200000        | 1      |
| 2.733333        | 1      | 3.333333        | 1      |
| 2.766667        | 1      | 3.466667        | 1      |

Table 8: Comparison of \( \text{RTO} \) and \( \text{MTO} \) of \((4, 4)\) S-boxes (I).

| \( \text{RTO} \) | Number | \( \text{MTO} \) | Number |
|-----------------|--------|-----------------|--------|
| 0.000000        | 1      | 3.266667        | 1      |
| 0.466667        | 1      | 3.466667        | 1      |
| 0.800000        | 1      | 3.266667        | 1      |
| 1.066667        | 1      | 3.066667        | 1      |
| 1.133333        | 1      | 3.466667        | 1      |
| 1.266667        | 1      | 3.333333        | 1      |
| 1.333333        | 3      | 3.133333        | 1      |
| 1.400000        | 1      | 3.466667        | 1      |
| 1.533333        | 1      | 3.466667        | 1      |
| 1.600000        | 1      | 3.466667        | 1      |
| 1.733333        | 2      | 3.466667        | 1      |
|                 |        | 3.133333        | 1      |
| 1.800000        | 4      | 3.266667        | 1      |
|                 |        | 3.333333        | 1      |
|                 |        | 3.466667        | 1      |
| 1.833333        | 1      | 3.133333        | 1      |
|                 |        | 3.133333        | 1      |
| 1.866667        | 5      | 3.266667        | 2      |
|                 |        | 3.466667        | 2      |
| 1.900000        | 1      | 3.333333        | 1      |
|                 |        | 3.133333        | 2      |
|                 |        | 3.200000        | 2      |
| 1.933333        | 8      | 3.266667        | 1      |
|                 |        | 3.333333        | 2      |
|                 |        | 3.533333        | 1      |
|                 |        | 3.200000        | 1      |
| 1.966667        | 3      | 3.266667        | 1      |
|                 |        | 3.466667        | 1      |
| 2.000000        | 2      | 3.333333        | 1      |
| 2.033333        | 1      | 3.200000        | 1      |
### Table 8: Continued.

| $RTO$   | Number | $MTO$   | Number |
|---------|--------|---------|--------|
| 2.066667 | 3      | 3.133333 | 2      |
|         |        | 3.266667 | 1      |
| 2.100000 | 2      | 3.466667 | 1      |
|         |        | 3.133333 | 2      |
|         |        | 3.200000 | 1      |
| 2.133333 | 6      | 3.266667 | 1      |
|         |        | 3.333333 | 1      |
|         |        | 3.466667 | 1      |
| 2.166667 | 2      | 3.333333 | 1      |
|         |        | 3.466667 | 1      |
| 2.200000 | 2      | 3.466667 | 1      |
|         |        | 3.133333 | 1      |
| 2.233333 | 1      | 3.066667 | 1      |
| 2.266667 | 6      | 3.333333 | 3      |
|         |        | 3.466667 | 2      |
|         |        | 3.133333 | 1      |
| 2.300000 | 5      | 3.200000 | 1      |
|         |        | 3.466667 | 3      |

### Table 9: Comparison of $RTO$ and $MTO$ of (4, 4) S-boxes (II).

| $RTO$   | Number | $MTO$   | Number |
|---------|--------|---------|--------|
| 2.333333 | 22     | 3.066667 | 4      |
|         |        | 3.133333 | 2      |
|         |        | 3.200000 | 2      |
|         |        | 3.266667 | 2      |
|         |        | 3.333333 | 7      |
|         |        | 3.466667 | 5      |
| 2.366667 | 15     | 3.066667 | 1      |
|         |        | 3.133333 | 2      |
|         |        | 3.200000 | 2      |
|         |        | 3.266667 | 6      |
|         |        | 3.333333 | 3      |
|         |        | 3.466667 | 1      |
| 2.400000 | 22     | 3.066667 | 1      |
|         |        | 3.133333 | 2      |
|         |        | 3.200000 | 4      |
|         |        | 3.266667 | 5      |
|         |        | 3.333333 | 4      |
|         |        | 3.466667 | 6      |
| 2.433333 | 21     | 3.066667 | 1      |
|         |        | 3.133333 | 2      |
|         |        | 3.200000 | 3      |
|         |        | 3.266667 | 6      |
|         |        | 3.333333 | 2      |
|         |        | 3.466667 | 6      |
|         |        | 3.533333 | 1      |
| 2.466667 | 30     | 3.066667 | 2      |
|         |        | 3.133333 | 10     |
|         |        | 3.200000 | 6      |
|         |        | 3.266667 | 4      |
|         |        | 3.333333 | 5      |
|         |        | 3.466667 | 2      |
|         |        | 3.533333 | 1      |
directly in the design of S-boxes, since a more natural option is to implement such a protection through some masking technique.

6. Conclusion
This paper further studies some unresolved problems related to the modified transparency order for \((n,m)\)-functions. Our result implies that \(RTO\) is less than or equal to \(MTO\) for any \((n,m)\)-function. In addition, a useful characterization of the modified transparency order is derived in terms of its tight bounds and its relation to other important cryptographic properties. These results show that the smaller the sum-of-squares indicator (or the nonlinearity and the algebraic immunity) of its coordinate, the bigger the modified transparency order. Although some results of \(MTO\) have been given in this paper, there are still few studies on \(MTO\). The design of \((n,m)\)-functions with small modified transparent order and good cryptographic indicators remains an open problem. At the same time, we will focus on the experimental verification of \((8,8)\)-functions for differential power attack and investigate the relationship between transparency order and confusion coefficient.

Data Availability
The data used to support the findings of this study are included within the article.

Conflicts of Interest
The authors declare that they have no conflicts of interest.

Acknowledgments
The first author was supported by the National Key R&D Program of China (nos. 2017YFB0802000 and 2017YFB0802004) and in part by the Sichuan Science and Technology Program (no. 2020JDJQ0076). The second author was supported in part by the National Natural Science
Foundation of China (61872103), Guangxi Science and Technology Foundation (Guike AB18281019), and Guangxi Natural Science Foundation (2019GXNSFA245004). The third author was supported in part by the National Cryptography Development Fund (grant no. MMJJ 20180223).

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," Advances in Cryptology – CRYPTO’99, Springer -Verlag, vol. 1666, pp. 388–397, , Berlin, Germany, 1999.

[2] S. Guillely, P. Hoogvorst, and R. Pacalet, "Differential power analysis model and some results, IFIP International Federation for Information Processing," in Smart Card Research and Advanced Applications VI -CARDIS 2004, J. J. Quisquater, P. Paradinas, Y. Deswarte, and A. E. Kalam, Eds., Kluwer Academic Publishers, New York, NY, USA, pp. 127–142, 2004.

[3] C. Beierle, J. Jean, S. Kölbl et al., “The SKINNY family of block ciphers and its low-latency variant MANTIS,” in Advances in Cryptology - CRYPTO 2016, M. Robshaw and I. Katz, Eds., vol. 9815Springer, Lecture Notes in Computer Science, , pp. 123–153, 2016.

[4] W. Fischer, B. M. Gammel, O. Kniffler, and J. Velten, “Differential power analysis of stream ciphers,” in Proceedings of the Topics in Cryptology – CT - RSA 2007, the Cryptographers Track at the RSA Conference 2007, vol. 257–270, San Francisco, CA, USA, February 5 -9, 2007.

[5] E. Prouff, “DPA attacks and S-boxes,” in Fast Software Encryption - FSE 2005, H. Handschuh and H. Gilbert, Eds., vol. 3557, pp. 424–441, Springer, Berlin, Germany, 2005.

[6] C. Carlet, “On highly nonlinear S-boxes and their inability to thwart DPA attacks,” in Progress in Cryptology – INDOCRYPT 2005, S. Maitra, C. E. Veni Madhavan, and R. Venkatesan, Eds., vol. 3795Springer, Lecture Notes in Computer Science, , pp. 49–62, 2005.

[7] L. Fan, Y. Zhou, and D. Feng, “A fast implementation of computing the transparency order of S – boxes,” in Proceedings of the The 9th International Conference for Young Computer Scientists (ICYCS 2008), pp. 206–211, IEEE Computer Society, Hunan, China, November 2008.

[8] Y. Fei, Q. Luo, and A. A. Ding, “A statistical model for DPA with novel algorithmic confusion analysis,” in Cryptographic Hardware and Embedded System -CHES 2012, E. Prouff and P. Schaumont, Eds., vol. 7428Springer, Lecture Notes in Computer Science, , pp. 233–250, 2012.

[9] Y. Fei, A. A. Ding, J. Lao, and L. Zhang, A Statistics – Based Fundamental Model for Side –channel Attack Analysis, Report 2014/152, IACR Cryptology ePrint Archive, Lyon, France, 2014.

[10] K. Chakraborty, S. Sarkar, S. Maitra, B. Mazumdar, D. Mukhopadhyay, and E. Prouff, “Redefining the transparency order,” Designs, Codes and Cryptography, vol. 82, no. 1 -2, pp. 95–115, 2017.

[11] S. Picek, B. Mazumdar, D. Mukhopadhyay, and L. Batina, "Modified transparency order property: solution or just another attempt," vol. 9354, pp. 210–227, in International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE), vol. 9354, , Springer International Publishing, Jaipur, India, October 2015.

[12] Q. Wang and P. Staničić, “Transparency order for boolean functions: analysis and construction,” Designs, Codes and Cryptography, vol. 87, no. 9, pp. 2043–2059, 2019.

[13] H. Li, Y. Zhou, J. Ming, G. Yang, and C. Jin, “The notion of transparency order, revisited,” The Computer Journal, vol. 63, no. 12, pp. 1915–1938, 2020.

[14] Y. Zhou, Y. Wei, and F. Zhang, “Measuring the sum-of-squares indicator of boolean functions in encryption algorithm for internet of things,” Security and Communication Networks, vol. 2019, no. 5, 15 pages, Article ID 1348639, 2019.

[15] P. Sarkar and S. Maitra, “Cross-correlation analysis of cryptographically useful boolean functions and S-boxes,” Theory of Computing Systems, vol. 35, no. 1, pp. 39–57, 2002.

[16] X. M. Zhang and Y. L. Zheng, “GAC – the criterion for global avalanche characteristics of cryptographic functions,” Journal of Universal Computer Science, vol. 1, no. 5, pp. 316–333, 1995.

[17] Y. Zhou, M. Xie, and G. Xiao, “On the global avalanche characteristics between two Boolean functions and the higher order nonlinearities,” Information Sciences, vol. 180, no. 2, pp. 256–265, 2010.

[18] Y. Zhou, W. Zhang, S. Zhu, and G. Xiao, “The global avalanche characteristics of two boolean functions and algebraic immunity,” International Journal of Computer Mathematics, vol. 89, no. 16, pp. 2165–2179, 2012.

[19] Y. Zheng and X. M. Zhang, “On plateaued functions,” IEEE Transactions on Information Theory, vol. 47, no. 3, pp. 1215–1223, 2011.

[20] C. Carlet, Boolean Functions for Cryptography and Error Correcting Codes, Y. Crama, L. Peter, and Hammer, Eds., Cambridge University Press, Cambridge, UK, 2010.

[21] M. R. Albrecht, B. Driessen, E. B. Kavun, G. Leander, C. Paar, and T. Yalçın, "Block ciphers - focus on the linear layer (feat. PRIDE)," Advances in Cryptology – CRYPTO 2014, Springer, Berlin, Germany, pp. 57–76, 2014.

[22] S. Banik, A. Bogdanov, T. Isobe et al., “Midori: a block cipher for low energy,” in Proceedings of the Advances in Cryptology – ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, pp. 411–436, Auckland, New Zealand, November 29, 2015.

[23] S. Banik, S. K. Pandey, T. Peyrin et al., “GIFT: a small present - towards reaching the limit of lightweight encryption,” in Proceedings of the Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, pp. 321–345, Taipei, Taiwan, September 25–28, 2017.

[24] A. Bogdanov, L. R. Knudsen, G. Leander et al., “PRESENT: an ultra – lightweight block cipher,” in Cryptographic Hardware and Embedded Systems – CHES 2007, 9th International Workshoppp. 450–466, Vienna, Austria, September 10 -13, 2007.

[25] J. Galbraith, A. Canteaut, T. Guney et al., “Prince – a low – latency block cipher for pervasive computing applications − extended abstract,” in Proceedings of the Advances in Cryptology – ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, pp. 208–225, Beijing, China, December 2–6, 2012.

[26] A. Marcos, J. R. Simplicio P. Barbuda et al., The MARVIN message authentication code and the LETTERSOUP authenticated encryption scheme,” Security and Communication Networks, vol. 2, no. 2, pp. 165–180, 2009.

[27] K. Shibutani, T. Isobe, H. Hiwatabi, A. Mitsuda, T. Akishita, and T. Shirai, “Piccolo: an ultra-lightweight b,” in Cryptographic Hardware and Embedded Systems – CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings, pp. 342–357, Springer, Berlin, Germany, 2011.
[28] W. Wu and L. Zhang, "LBlock: a lightweight block cipher," in Applied Cryptography and Network Security - ACNS 2011, J. Lopez and G. Tsudik, Eds., vol. 6715Springer, Lecture Notes in Computer Science, , pp. 327–344, 2011.

[29] G. Leander and A. Poschmann, On the Classification of 4 Bit S-boxes, Arithmetic of Finite Fields, pp. 159–176, Springer, Berlin, Germany, 2007.

[30] C. D. E. Canniere, Analysis and design of symmetric encryption algorithms, Katholieke Universiteit Leuven, Leuven, Belgium, PH.D, 2007.