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

Academic Editor: Angel M. Del Rey

Copyright © 2021 Yu Zhou et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

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 \(TO\)) based on the autocorrelation coefficients for \((n, m)\)-functions. He obtained that S-boxes with smaller \(TO\) have higher DPA resilience and deduced the tightness of the upper bound and the lower bound on the \(TO\). 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.

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

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

In this article, we focus on some unresolved problems related to both $\text{RTO}$ and $\text{MTO}$. Firstly, we give the relationship between $\text{MTO}$ and $\text{RTO}$, and this result implies that $\text{MTO}(F) \geq \text{RTO}(F)$ for any $(n, m)$-functions $F$. We also obtain the upper bound and the lower bound on $\text{MTO}$. To design good S-boxes with respect to the $\text{MTO}$ [13], we deduce some important connections between $\text{MTO}$ 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 $\text{MTO}$, whereas a higher nonlinearity (or algebraic immunity) of the coordinate functions of a given $(n, m)$-function also implies a larger $\text{MTO}$ (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 $\text{MTO}$ and $\text{RTO}$ for $(4, 4)$ S-boxes which are commonly used in some lightweight block ciphers, it implies that $\text{MTO}$ is better than $\text{RTO}$ 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 $\text{MTO}(F)$ 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 $B_n$ be the set of $n$-variable Boolean functions. We denote by $\oplus$ the addition modulo two performed in $F_2$ and the vector space $F_2^n$. The support of a Boolean function $f \in B_n$ is defined as $\text{supp}(f) = \{x_1, \ldots, x_n\} \in F_2^n[f(x_1, \ldots, x_n) = 1]$. The Hamming weight of $f$ is denoted by $w(f)$ and corresponds to the cardinality of its support $w(f) = |\text{supp}(f)|$. A Boolean function $f$ is said to be balanced if its truth table contains equal number of ones and zeros, i.e., $w(f) = 2^{n-1}$. 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 $F_2^n$.

Definition 1. Let $f \in B_n$. The Walsh spectrum of $f$ is defined by

$$\mathcal{F}(f \oplus \varphi_a) = \sum_{x \in F_2^n} (-1)^f(x)\varphi_a(x), \quad a \in F_2^n,$$

where $\varphi_a(x) = a \cdot x = a_1x_1 \oplus \cdots \oplus a_nx_n$, $x = (x_1, x_2, \ldots, x_n)$, $a = (a_1, a_2, \ldots, a_n)$. The nonlinearity of $f$ can be computed using

$$N_f = 2^{n-1} - \frac{1}{2} \max_{a \in F_2^n} |\mathcal{F}(f \oplus \varphi_a)|.$$  

Let $f, g \in B_n$. The cross-correlation function between $f$ and $g$ is defined by

$$\Delta_{f,g}(\alpha) = \sum_{x \in F_2^n} (-1)^{f(x)\oplus g(x)\oplus \alpha}, \quad \alpha \in F_2^n.$$

In particular, when $f = g$, then the autocorrelation function of $f \in B_n$ is given by

$$\Delta_f(\alpha) = \sum_{x \in F_2^n} (-1)^{f(x)\oplus f(x)\oplus \alpha}, \quad \alpha \in F_2^n.$$

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

Two functions $f, g \in B_n$ are said to be perfectly uncorrelated if $\Delta_{f,g}(\alpha) = 0$, for any $\alpha \in F_2^n$. From [15], if $f$ and $g$ are perfectly uncorrelated, then $\mathcal{F}(f \oplus \varphi_a)\mathcal{F}(g \oplus \varphi_a) = 0$ for any $\alpha \in F_2^n$.

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

$$\sigma_f = \sum_{\alpha \in F_2^n} \left|\Delta_f(\alpha)\right|^2,$$

$$\Delta_f = \max_{\alpha \in F_2^n, \alpha \neq 0^n} \left|\Delta_f(\alpha)\right|.$$
In 2010, Zhou et al. [17] generalized GAC and gave the global avalanche characteristics between two Boolean functions $f, g \in \mathbb{B}_n$;
\[
\sigma_{f,g} = \sum_{a \in \mathbb{F}_2^n} \left[ \Delta_{f,g}(a) \right]^2,
\]
\[
\Delta_{f,g} = \max_{a \in \mathbb{F}_2^n} \left| \Delta_{f,g}(a) \right|.
\] (6)

For two positive integers $n$ and $m$, a function $F: \mathbb{F}_2^n \rightarrow \mathbb{F}_m^n$ 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 nonzero $v \in \mathbb{F}_2^n$, the Boolean function $v \cdot F$ 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 transparency order [10] are for balanced $(n, m)$-functions, 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
\[
\mathcal{RT}(F) = \max_{\beta \in \mathbb{F}_2^m} \left\{ m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^n} \sum_{j=1}^{m} (-1)^{\beta_j} \Delta_{f_i,f_j}(a) \right\},
\] (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
\[
\mathcal{MT}(F) = \max_{\beta \in \mathbb{F}_2^m} \left\{ m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^n} \sum_{j=1}^{m} (-1)^{\beta_j} \Delta_{f_i,f_j}(a) \right\},
\] (8)

Note that
\[
(-1)^{\beta_j} \Delta_{f_i,f_j}(a) = \Delta_{f_{i,\beta_j},f_{j,\beta_j}}(a),
\] (9)
and for research convenience, let
\[
\Gamma_F^\beta = m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^n} \sum_{j=1}^{m} \Delta_{f_{i,\beta_j},f_{j,\beta_j}}(a).
\] (10)
Thus,
\[
\mathcal{MT}(F) = \max_{\beta \in \mathbb{F}_2^m} \Gamma_F^\beta.
\] (11)

### 3. Bounds on the Modified Transparency Order

Based on Definition 4, a lower bound on $\mathcal{MT}(F)$ 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 $\mathcal{MT}(F)$, we firstly give a relationship between $\mathcal{MT}(F)$ and $\mathcal{RT}(F)$.

**Lemma 1** (see [17]). Let $f, g \in \mathbb{B}_n$. Then,
\[
\sum_{a \in \mathbb{F}_2^n} \Delta_{f,g}(a) = (2^n - 2\text{wt}(f))(2^n - 2\text{wt}(g)).
\] (12)

**Theorem 1.** Let $F = (f_1, \ldots, f_m)$ be an $(n, m)$-function. Then,
\[
\mathcal{MT}(F) \geq \mathcal{RT}(F).
\] (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
\[
\sum_{j=1}^m m \sum_{j=1}^m (-1)^{\beta_j} \Delta_{f_i,f_j}(a) \leq \sum_{j=1}^m m \sum_{j=1}^m (-1)^{\beta_j} \Delta_{f_i,f_j}(a), \quad a \in \mathbb{F}_2^n.
\] (14)
For any $a \in \mathbb{F}_2^n$, we have
\[
m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^n} \sum_{j=1}^m m \sum_{j=1}^m (-1)^{\beta_j} \Delta_{f_i,f_j}(a) \geq
\sum_{j=1}^m m \sum_{j=1}^m (-1)^{\beta_j} \Delta_{f_i,f_j}(a)
\] (15)
Based on the above equation, we have $\mathcal{MT}(F) \geq \mathcal{RT}(F)$.

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

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

In the following, we give a tight upper bound and a tight lower bound on $\mathcal{MT}(F)$ 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
\[
0 \leq \mathcal{MT}(F) \leq m.
\] (16)

**Proof.** On the one hand, from Definition 4 and Lemma 1, we have
\[
\gamma^\beta_F = m - \frac{1}{2^{2m} - 2^n} \sum_{a \in F_2^n} \left| \sum_{j=1}^{m} \sum_{i=1}^{m} \Delta_{f, \theta_i, f, \theta_j}(a) \right|
\]

\[
= m - \frac{1}{2^{2m} - 2^n} \sum_{a \in F_2^n} \left| \sum_{j=1}^{m} \Delta_{f, \theta_i, f, \theta_j}(a) + \cdots + \Delta_{f, \theta_{m}, f, \theta_j}(a) \right|
\]

\[
\leq m - \frac{1}{2^{2m} - 2^n} \left| \sum_{j=1}^{m} \sum_{i=1}^{m} \Delta_{f, \theta_i, f, \theta_j}(a) + \cdots + \Delta_{f, \theta_{m}, f, \theta_j}(a) \right|
\]

\[
= m - \frac{1}{2^{2m} - 2^n} \left| \sum_{j=1}^{m} \sum_{i=1}^{m} \Delta_{f, \theta_i, f, \theta_j}(a) + \cdots + \Delta_{f, \theta_{m}, f, \theta_j}(a) \right|
\]

\[
= m - \frac{1}{2^{2m} - 2^n} \left| \sum_{j=1}^{m} \left( (-1)^{\beta_i \theta_j} \left( 2^n - 2^{wt(f_i)} \right) \left( 2^n - 2^{wt(f_j)} \right) - \Delta_{f, f_j}(0^n) \right) + (-1)^{\beta_i \theta_j} \right|
\]

\[
\cdot \left( 2^n - 2^{wt(f_i)} \right) \left( 2^n - 2^{wt(f_j)} \right) - \Delta_{f, f_j}(0^n) \right)
\]

\[
+ \cdots + (-1)^{\beta_i \theta_j} \left( 2^n - 2^{wt(f_m)} \right) \left( 2^n - 2^{wt(f_j)} \right) - \Delta_{f, f_j}(0^n) \right).
\]

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 \( \Delta_{f, f_j}(0^n) = 2^{2n} - 2^{\text{wt}(f_i \oplus f_j)} = 0 \) and \( 2^{2n} - 2^{\text{wt}(f_k)} = 0 \) for any \( 1 \leq i < j \leq m, \leq k \leq m. \)

Thus, \( \gamma^\beta_F \leq m \), that is, \( \mathcal{O}(F) \leq m. \)

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 \( a \in F_2^n \) and \( 1 \leq i \neq j \leq m. \)

From Definition 4, we have

\[
\gamma^\beta_F = m - \frac{1}{2^{2m} - 2^n} \sum_{a \in F_2^n} \left| \sum_{j=1}^{m} \sum_{i=1}^{m} \Delta_{f, \theta_i, f, \theta_j}(a) \right|
\]

\[
= m - \frac{1}{2^{2m} - 2^n} \sum_{a \in F_2^n} \left| \Delta_{f_i}(a) + \Delta_{f_j}(a) + \cdots + \Delta_{f_m}(a) \right|
\]

\[
\geq m - \frac{1}{2^{2m} - 2^n} \sum_{a \in F_2^n} \left| \Delta_{f_i}(a) \right| + \left| \Delta_{f_j}(a) \right| + \cdots + \left| \Delta_{f_m}(a) \right|
\]

\[
(18)
\]

By Cauchy's inequality and \( 2^{2n} \leq \sigma_{f_i} = \sum_{a \in F_2^n} |\Delta_{f_i}(a)|^2 \leq 2^{3n} \) for any \( 1 \leq i \leq m \) in [16], we have

\[
2^{3n} - 2^{2n} = \sum_{a \in F_2^n} |\Delta_{f_i}(a)|^2 \geq \left( \sum_{a \in F_2^n} |\Delta_{f_i}(a)| \right)^2
\]

\[
\geq \frac{\left( \sum_{a \in F_2^n} |\Delta_{f_i}(a)| \right)^2}{2^n - 1}.
\]

Thus,

\[
\sum_{a \in F_2^n} |\Delta_{f_i}(a)| \leq 2^n (2^n - 1), \quad 1 \leq i \leq m.
\]

From equation (20), we have

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

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

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

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

Then, \( f_1 \) and \( f_2 \) are bent functions. We know \( \Delta_{f_1}(a) = 0 \) and \( \Delta_{f_2, f_j}(a) = 0 \) for any \( a \in F_2^m \) and \( 1 \leq i \neq j \leq m. \) We have

\[
\gamma^\beta_F = m - \frac{1}{2^{2m} - 2^n} \sum_{a \in F_2^n} \left| \sum_{j=1}^{m} \sum_{i=1}^{m} \Delta_{f, \theta_i, f, \theta_j}(a) \right|
\]

\[
= m - \frac{1}{2^{2m} - 2^n} \sum_{a \in F_2^n} \left| \Delta_{f_1}(a) \right| + \left| \Delta_{f_2}(a) \right| + \cdots + \left| \Delta_{f_m}(a) \right|
\]

\[
(23)
\]

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

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

\[
f_1(x) = x_1 \oplus x_2, \quad f_2(x) = x_3 \oplus x_4.
\]

Then, \( F \) is balanced \((n = 4, m = 2)\). We know \( |\Delta_{f_1}(a)| = 2^n \) and \( \Delta_{f_2, f_j}(a) = 0 \) for any \( a \in F_2^m \) and \( 1 \leq i \neq j \leq m. \) Then, we have
Theorem 3. Let \( F = (f_1, \ldots, f_m) \) be a balanced \((n, m)\)-function. Then,
\[
\mathcal{MT}_0(F) \geq m \left[ 1 - \frac{\sum_{j=1}^{m} \sqrt{\sigma_{f_j}}}{2^n\sqrt{2^n - 1}} \right].
\]  
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
\[
\Gamma_\beta^F = m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^n} \left| \sum_{j=1}^{m} \Delta_{f_\beta_j}(a) \right|
\]
\[
= m - \frac{m2^n(2^n - 1)}{2^{2n} - 2^n}
\]
\[
= 0,
\]
and thus \( \mathcal{MT}_0(F) = 0 \).

Remark 2. Corollary 1 is a special case of Theorem 2. It also shows that both the upper bound and the lower bound on \( \mathcal{MT}_0 \) can be reached.

4. The Relationships between \( \mathcal{MT}_0 \) and Some Cryptographic Properties

In this section, we use the sum-of-squares indicator to establish some links between \( \mathcal{MT}_0 \) and some cryptographic indicators. These links can help us understand \( \mathcal{MT}_0 \) more deeply and lay a foundation for designing and analyzing S-boxes. In the following, we give a relationship between \( \mathcal{MT}_0 \) and the sum-of-squares indicator, and this result is the basic of Corollaries 3 and 4.

4.1. The Relationships between \( \mathcal{MT}_0 \) and the Sum-of-Squares Indicator

Theorem 3. Let \( F = (f_1, \ldots, f_m) \) be a balanced \((n, m)\)-function. Then,
\[
\mathcal{MT}_0(F) \geq m \left[ 1 - \frac{\sum_{j=1}^{m} \sqrt{\sigma_{f_j}}}{2^n\sqrt{2^n - 1}} \right].
\]  
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
\[
\Gamma_\beta^F \geq m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^n} \left| \sum_{j=1}^{m} \Delta_{f_\beta_j}(a) \right|
\]
\[
\geq m - \frac{1}{2^{2n} - 2^n} \left[ (2^n - 1)m \sum_{j=1}^{m} \sigma_{f_j} \right]^{1/2}
\]
\[
= m \left[ 1 - \frac{\sum_{j=1}^{m} \sqrt{\sigma_{f_j}}}{2^n\sqrt{2^n - 1}} \right].
\]  

Furthermore, we have
\[
\Gamma_\beta^F \geq \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^n} \sum_{j=1}^{m} \Delta_{f_\beta_j}(a)
\]
\[
\geq m \left[ 1 - \frac{\sum_{j=1}^{m} \sqrt{\sigma_{f_j}}}{2^n\sqrt{2^n - 1}} \right].
\]  

Because \( \sigma_{f,g} \leq \sqrt{\sigma_f \sigma_g} \) for any \( f, g \in \mathbb{B}_n \) [18], we have
\[
\Gamma_\beta^F \geq \frac{1}{2^{2n} - 2^n} \left[ \sum_{j=1}^{m} \frac{\sigma_{f_j}^{1/2}}{\sqrt{2^n - 1}} \right]
\]
\[
= m \left[ 1 - \frac{\sum_{j=1}^{m} \sqrt{\sigma_{f_j}}}{2^n\sqrt{2^n - 1}} \right].
\]
From Definition 4, we know that
\[ MTF(F) = \max_{\beta \in F^2} \beta. \] (33)
Thus,
\[ MTF(F) \geq 1^\beta_F \geq m \left[ 1 - \frac{\sum_{i=1}^{m} |\phi_{j_i}|}{2^n(2^n - 1)} \right]. \] (34)

**Remark 3.** Theorem 3 gives one relationship between \( MTF(F) \) and \( \sigma_f(1 \leq i \leq m) \), which implies that the smaller \( \sigma_f(1 \leq i \leq m) \), the bigger the \( MTF(F) \).

Based on Theorem 3, we give some lower bounds on \( MTF \) by nonlinearity and algebraic immunity.

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

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

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

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

**Corollary 4.** Let \( F = (f_1, \ldots, f_m) \) be a balanced \((n,m)\)-function. Then,
\[ MTF(F) \geq m \left[ 1 - \frac{1}{\sqrt{2^n(2^n - 1)}} \sqrt{AB} \right], \] (37)
where \( A = \sum_{i=1}^{m} \left( 2^n - 4 \sum_{k=0}^{n} \left( n - 1 \right) \binom{n-1}{k} \right) \), \( B = \sum_{j=1}^{m} \binom{n}{j} \).

**Proof.** Carlet [20] obtained \( N_{f_i} \geq 2^{\sum_{j=0}^{n} \binom{n-1}{j} - 1} \binom{n-1}{i} \) for \( 1 \leq i \leq m \), and thus this result is easily proved. \( \square \)

**Remark 4.** From Corollaries 3 and 4, we have
(1) The larger the \( N_{f_i} \) (or \( \text{AI}(f_i) \)) \((1 \leq i \leq m)\), the larger the \( MTF(F) \).
(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 \( MTF \) and Hamming Weight.

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

**Theorem 4.** Let \( F = (f_1, \ldots, f_m) \) be an \((n,m)\)-function and \( \text{wt}(f_i) = 2^{n-1} \) \((1 \leq i \leq m)\). Then, for any \( \beta = (\beta_1, \beta_2, \ldots, \beta_m) \in F^m \),
\[ MTF(F) \leq m - \frac{\sum_{j=1}^{m} \sum_{i=1}^{m} (-1)^{\beta_i \beta_j} \text{wt}(f_i \oplus f_j)}{2^{2n} - 2^n}. \] (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
\[ \Gamma^g_f = m - \sum_{a \in F^*_2} \left[ \sum_{j=1}^m \sum_{i=1}^{m} \Delta_f \beta_j f, \beta_j (a) \right] \]
\[ \leq m - \frac{1}{2^{2n} - 2^n} \sum_{j=1}^m \left[ \sum_{i=1}^{m} \left[ \sum_{a \in F^*_2} \Delta_f \beta_j f, \beta_j (a) \right] \right] \]
\[ = m - \frac{1}{2^{2n} - 2^n} \sum_{j=1}^m \left[ \sum_{i=1}^{m} \left[ \sum_{a \in F^*_2} \left( \Delta_f \beta_j f, \beta_j (a) \right) \right] \right] \]
\[ = m - \frac{1}{2^{2n} - 2^n} \sum_{j=1}^m \left[ \sum_{i=1}^{m} \left[ \sum_{a \in F^*_2} \left( \Delta_f \beta_j f, \beta_j (0^i) \right) \right] \right] \]
\[ = m - \frac{1}{2^{2n} - 2^n} \sum_{j=1}^m \left[ \sum_{i=1}^{m} \left[ \sum_{a \in F^*_2} \left( \Delta_f \beta_j f, \beta_j (0^i) \right) \right] \right] \]
\[ = m - \frac{1}{2^{2n} - 2^n} \sum_{j=1}^m \left[ \sum_{i=1}^{m} \left[ \sum_{a \in F^*_2} \left( \Delta_f \beta_j f, \beta_j (0^i) \right) \right] \right] \]

which proves the result. \(\square\)

Remark 5. If \(|f| \oplus |f_j| = 2^{n-1}\) for any \(1 \leq i \neq j \leq m\), then \(\mathcal{M} \mathcal{T} \mathcal{O}(F) \leq m - (m/2^n - 1)\). This implies that \(\mathcal{M} \mathcal{T} \mathcal{O}(F) \leq m - (m/2^n - 1)\) 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,
\[ 0 \leq \mathcal{M} \mathcal{T} \mathcal{O}(F) \leq m - \frac{m}{2^n - 1}. \] (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 \(\mathcal{M} \mathcal{T} \mathcal{O}\).

Corollary 6. Let \(f \in \mathbb{B}_n\). Then,
1. \(\mathcal{M} \mathcal{T} \mathcal{O}(f) \geq 1 - \sqrt{(2^n - 1/2^n - 2^n)}\)
2. \(\mathcal{M} \mathcal{T} \mathcal{O}(f) \geq 1 - \sqrt{(2^n - 2^n/2^n - 2^n)}\)
3. \(\mathcal{M} \mathcal{T} \mathcal{O}(f) \geq 1 - \sqrt{(2^n - N_j)^2 - 2^n/2^n - 2^n)}\)
4. \(\mathcal{M} \mathcal{T} \mathcal{O}(f) \leq 1 - \sqrt{(2^n - 2wt(f))^2 - 2^n/2^n - 2^n)}\)

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 \(\mathcal{M} \mathcal{T} \mathcal{O}\) by the nonlinearity of Boolean function; here we give the lower bounds on \(\mathcal{M} \mathcal{T} \mathcal{O}\) by the nonlinearity, the sum-of-squares indicator, and the maximum absolute of Walsh 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 \(\mathcal{R} \mathcal{T} \mathcal{O}\) or \(\mathcal{M} \mathcal{T} \mathcal{O}\) 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. \(\mathcal{R} \mathcal{T} \mathcal{O}\) and \(\mathcal{M} \mathcal{T} \mathcal{O}\) of Some Known S-Boxes in Well-Known Encryption Algorithms. We give the \(\mathcal{R} \mathcal{T} \mathcal{O}\) and \(\mathcal{M} \mathcal{T} \mathcal{O}\) 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 \(\mathcal{R} \mathcal{T} \mathcal{O} \leq \mathcal{M} \mathcal{T} \mathcal{O}\) for a given S-box. This is consistent with Theorem 1.

5.2. The \(\mathcal{M} \mathcal{T} \mathcal{O}\) 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.
Table 1: $MTO$ and $FTO$ of well-known S-boxes.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>S-box</th>
<th>$FTO$</th>
<th>$MTO$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pride [21]</td>
<td>048F15E927ACBD63</td>
<td>2.466667</td>
<td>3.133333</td>
</tr>
<tr>
<td>Midori [22]</td>
<td>CAD3EBF789150246</td>
<td>2.166667</td>
<td>3.066667</td>
</tr>
<tr>
<td>Gift [23]</td>
<td>1A4C63F92DB7508E</td>
<td>2.200000</td>
<td>3.066667</td>
</tr>
<tr>
<td>MANTIS [3]</td>
<td>CAD3EBF789150246</td>
<td>2.166667</td>
<td>3.066667</td>
</tr>
<tr>
<td>PRESENT [24]</td>
<td>C56B90AD3EF84712</td>
<td>2.466667</td>
<td>3.266667</td>
</tr>
<tr>
<td>Marvin [26]</td>
<td>021B83ED46F5C79A</td>
<td>2.666667</td>
<td>3.200000</td>
</tr>
<tr>
<td>Piccolo [27]</td>
<td>E4B238091A7F6C5D</td>
<td>2.566667</td>
<td>3.200000</td>
</tr>
<tr>
<td></td>
<td>9F0D4AB12376C5</td>
<td>2.566667</td>
<td>3.333333</td>
</tr>
<tr>
<td></td>
<td>4BE9FDDAC562813</td>
<td>2.566667</td>
<td>3.333333</td>
</tr>
<tr>
<td></td>
<td>1E7CFCDB59324BA</td>
<td>2.566667</td>
<td>3.333333</td>
</tr>
<tr>
<td></td>
<td>768B0F3E9A6D5241</td>
<td>2.566667</td>
<td>3.333333</td>
</tr>
<tr>
<td></td>
<td>ESF072CD1849BA63</td>
<td>2.566667</td>
<td>3.333333</td>
</tr>
<tr>
<td>Lblock [28]</td>
<td>2DBC6E097A631845</td>
<td>2.566667</td>
<td>3.333333</td>
</tr>
<tr>
<td></td>
<td>B94E0F6AD5657C12</td>
<td>2.566667</td>
<td>3.333333</td>
</tr>
<tr>
<td></td>
<td>DAF0E49B18375C6</td>
<td>2.566667</td>
<td>3.333333</td>
</tr>
<tr>
<td></td>
<td>87E5F06DC9A2413</td>
<td>2.566667</td>
<td>3.333333</td>
</tr>
<tr>
<td></td>
<td>B5F072D481CEA36</td>
<td>2.566667</td>
<td>3.333333</td>
</tr>
</tbody>
</table>

Table 2: Representatives for 16 optimal $(4,4)$ S-boxes [29].

<table>
<thead>
<tr>
<th>Class</th>
<th>$(4,4)$ S-boxes</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_1$</td>
<td>0, 1, 2, 13, 4, 7, 15, 6, 8, 11, 12, 9, 3, 14, 10, 5</td>
</tr>
<tr>
<td>$G_2$</td>
<td>0, 1, 2, 13, 4, 7, 15, 6, 8, 11, 14, 3, 5, 9, 10, 12</td>
</tr>
<tr>
<td>$G_3$</td>
<td>0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 5, 3, 10, 14, 11, 9</td>
</tr>
<tr>
<td>$G_4$</td>
<td>0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 9, 11, 10, 14, 5, 3</td>
</tr>
<tr>
<td>$G_5$</td>
<td>0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 11, 9, 10, 14, 3, 5</td>
</tr>
<tr>
<td>$G_6$</td>
<td>0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 11, 9, 10, 14, 5, 3</td>
</tr>
<tr>
<td>$G_7$</td>
<td>0, 1, 2, 13, 4, 7, 15, 6, 8, 12, 11, 9, 10, 3, 5</td>
</tr>
<tr>
<td>$G_8$</td>
<td>0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 9, 5, 10, 11, 3, 12</td>
</tr>
<tr>
<td>$G_9$</td>
<td>0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 11, 3, 5, 9, 10, 12</td>
</tr>
<tr>
<td>$G_{10}$</td>
<td>0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 11, 10, 9, 3, 12</td>
</tr>
<tr>
<td>$G_{11}$</td>
<td>0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 11, 10, 5, 9, 12, 3</td>
</tr>
<tr>
<td>$G_{12}$</td>
<td>0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 11, 10, 9, 3, 12</td>
</tr>
<tr>
<td>$G_{13}$</td>
<td>0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 12, 9, 11, 5, 10, 3</td>
</tr>
<tr>
<td>$G_{14}$</td>
<td>0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 12, 11, 3, 9, 5, 10</td>
</tr>
<tr>
<td>$G_{15}$</td>
<td>0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 12, 11, 9, 3, 10, 5</td>
</tr>
</tbody>
</table>

By Proposition 3 in [13], we know that $MTO$ means affine invariant only under certain affine transformations which are based on $S_2(x) = S_1(A \cdot x+c)d \oplus d$, where $S_1, S_2$ are two $(n, n)$ S-boxes, and $A$ is an invertible $n \times n$ matrix. This means that $MTO$ may change under different affine transformations $S_2(x) = A \cdot S_1(x)$, and we only consider this case in the following. From the finite field, we know that the number of the invertible $n \times n$ matrix in $F_2^n$ is $q^{n(n-1)/2} \prod_{i=1}^{n} (q^{n-i} - 1)$. Thus, the number of the invertible $4 \times 4$ matrix in $F_2$ is $0.166667 \prod_{i=1}^{4} (q-1)$. The number of the affine S-boxes (A+S) of one S-box (G) is 20160, where G is a 4-bit S-box and A is an invertible $4 \times 4$ matrix.

At the same time, bounds and the frequency distribution of $MTO$ are given for all affine transformations of 16 optimal classes in [13]. But from these data, we cannot find out what the distribution of $G_i$, $i = 0, 1, \ldots, 15$ is, and how many s boxes there are in each distribution value. For example, in the algorithm design, we want to know the exact value of $MTO$, not the range of $MTO$ in [13]. Therefore, we need to give specific data values for every $G_i$ ($i = 0, 1, \ldots, 15$), and Tables 3-6 provide support for us to select S-box. Meanwhile, these data further improve the data in [13].

In Table 3, we calculate $MTO$ of 20160 S-boxes $A \cdot G_i$ for $G_i$ ($0 \leq i \leq 15$). We find the following facts:

1. The $MTO$ of $A \cdot G_i$ has 11 values, if $i = 0, 1, 8, 15$.
2. The $MTO$ of $A \cdot G_i$ has 10 values, if $i = 2$.
3. The $MTO$ of $A \cdot G_i$ has 9 values, if $i = 4, 7, 9, 10, 13, 14$.
4. The $MTO$ of $A \cdot G_i$ has 8 values, if $i = 6, 11$.
5. The $MTO$ of $A \cdot G_i$ has 7 values, if $i = 5, 12$.
6. The $MTO$ of $A \cdot G_i$ has 4 values, if $i = 3$.

Furthermore, we give the corresponding mean and variance in each optimal class in Table 4.

The mean value of $MTO$ for $A \cdot G_i$ ($i = 0, 1, 2, \ldots, 15$) belongs to the range of $[3.195714, 3.264286]$, and the variance belongs to range of $[0.007448, 0.021143]$. The distribution of its value is concentrated in a relatively small interval.

Especially, we get the detailed distribution of $MTO$ of $A'G_0$ and $A'G_1$ 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 $2.666667 \leq RTO(F) \leq 3.533333$, but $0 \leq RTO(F) \leq 2.766667$ 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 Theorem 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 MTO of affine equivalent S-boxes of $G_3$.

<table>
<thead>
<tr>
<th>Class</th>
<th>MTO ($A \circ G_3$)</th>
<th>Number</th>
<th>Per (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3.133333</td>
<td>7200</td>
<td>35.7143</td>
</tr>
<tr>
<td>2</td>
<td>3.200000</td>
<td>3960</td>
<td>19.6429</td>
</tr>
<tr>
<td>3</td>
<td>3.266667</td>
<td>1800</td>
<td>8.9286</td>
</tr>
<tr>
<td>4</td>
<td>3.333333</td>
<td>7200</td>
<td>35.7143</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>RTO</th>
<th>Number</th>
<th>MTO</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.633333</td>
<td>9</td>
<td>2.866667</td>
<td>2</td>
</tr>
<tr>
<td>2.666667</td>
<td>7</td>
<td>3.133333</td>
<td>1</td>
</tr>
<tr>
<td>2.700000</td>
<td>1</td>
<td>3.200000</td>
<td>1</td>
</tr>
<tr>
<td>2.733333</td>
<td>1</td>
<td>3.333333</td>
<td>1</td>
</tr>
<tr>
<td>2.766667</td>
<td>1</td>
<td>3.466667</td>
<td>1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>RTO</th>
<th>Number</th>
<th>MTO</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.000000</td>
<td>1</td>
<td>3.266667</td>
<td>1</td>
</tr>
<tr>
<td>0.466667</td>
<td>1</td>
<td>3.466667</td>
<td>1</td>
</tr>
<tr>
<td>0.800000</td>
<td>1</td>
<td>3.266667</td>
<td>1</td>
</tr>
<tr>
<td>1.066667</td>
<td>1</td>
<td>3.066667</td>
<td>1</td>
</tr>
<tr>
<td>1.133333</td>
<td>1</td>
<td>3.466667</td>
<td>1</td>
</tr>
<tr>
<td>1.266667</td>
<td>1</td>
<td>3.333333</td>
<td>1</td>
</tr>
<tr>
<td>1.333333</td>
<td>3</td>
<td>3.133333</td>
<td>1</td>
</tr>
<tr>
<td>1.400000</td>
<td>1</td>
<td>3.466667</td>
<td>1</td>
</tr>
<tr>
<td>1.533333</td>
<td>1</td>
<td>3.466667</td>
<td>1</td>
</tr>
<tr>
<td>1.600000</td>
<td>1</td>
<td>3.466667</td>
<td>1</td>
</tr>
<tr>
<td>1.733333</td>
<td>2</td>
<td>3.466667</td>
<td>1</td>
</tr>
<tr>
<td>1.800000</td>
<td>4</td>
<td>3.333333</td>
<td>1</td>
</tr>
<tr>
<td>1.833333</td>
<td>1</td>
<td>3.133333</td>
<td>1</td>
</tr>
<tr>
<td>1.866667</td>
<td>5</td>
<td>3.266667</td>
<td>2</td>
</tr>
<tr>
<td>1.900000</td>
<td>1</td>
<td>3.333333</td>
<td>1</td>
</tr>
<tr>
<td>1.933333</td>
<td>8</td>
<td>3.266667</td>
<td>1</td>
</tr>
<tr>
<td>1.966667</td>
<td>3</td>
<td>3.266667</td>
<td>1</td>
</tr>
<tr>
<td>2.000000</td>
<td>2</td>
<td>3.333333</td>
<td>1</td>
</tr>
<tr>
<td>2.033333</td>
<td>1</td>
<td>3.200000</td>
<td>1</td>
</tr>
</tbody>
</table>
Table 8: Continued.

<table>
<thead>
<tr>
<th>RTO</th>
<th>Number</th>
<th>MTO</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.066667</td>
<td>3</td>
<td>3.133333</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.266667</td>
<td>1</td>
</tr>
<tr>
<td>2.100000</td>
<td>3</td>
<td>3.133333</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.200000</td>
<td>1</td>
</tr>
<tr>
<td>2.133333</td>
<td>6</td>
<td>3.266667</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.333333</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.466667</td>
<td>1</td>
</tr>
<tr>
<td>2.166667</td>
<td>2</td>
<td>3.333333</td>
<td>1</td>
</tr>
<tr>
<td>2.200000</td>
<td>2</td>
<td>3.466667</td>
<td>1</td>
</tr>
<tr>
<td>2.233333</td>
<td>1</td>
<td>3.133333</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.066667</td>
<td>1</td>
</tr>
<tr>
<td>2.266667</td>
<td>6</td>
<td>3.333333</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.466667</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.133333</td>
<td>1</td>
</tr>
<tr>
<td>2.300000</td>
<td>5</td>
<td>3.200000</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.466667</td>
<td>3</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>RTO</th>
<th>Number</th>
<th>MTO</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.333333</td>
<td>22</td>
<td>3.066667</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.133333</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.200000</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.266667</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.333333</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.466667</td>
<td>5</td>
</tr>
<tr>
<td>2.366667</td>
<td>15</td>
<td>3.066667</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.133333</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.200000</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.266667</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.333333</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.466667</td>
<td>1</td>
</tr>
<tr>
<td>2.400000</td>
<td>22</td>
<td>3.066667</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.133333</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.200000</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.266667</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.333333</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.466667</td>
<td>6</td>
</tr>
<tr>
<td>2.433333</td>
<td>21</td>
<td>3.066667</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.133333</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.200000</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.266667</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.333333</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.466667</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.533333</td>
<td>1</td>
</tr>
<tr>
<td>2.466667</td>
<td>30</td>
<td>3.066667</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.133333</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.200000</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.266667</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.333333</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.466667</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.533333</td>
<td>1</td>
</tr>
</tbody>
</table>
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...
References


