On characterization of transparency order for (n, m)-functions

Yu Zhou[1], Yongzhuang Wei[2], Hailong Zhang[3], Luyang Li[4], Enes Pasalic[5], and Wenling Wu[6]

[1] Science and Technology on Communication Security Laboratory, Chengdu, 610041, China.
zhouyu.zhy@tom.com
[2] Guilin University of Electronic Technology, Guilin, 541004, China.
walker_wei@msn.com
[3] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 100093, China.
zhanghailong@iie.ac.cn
[4] National Engineering Laboratory for Wireless Security, Xi'an University of Post and Telecommunications, Xi'an, 710061, China.
luyang_li@foxmail.com
[5] University of Primorska, FAMNIT & IAM, Koper, Slovenia.
enes.pasalic6@gmail.com
[6] TCA Laboratory, SKLCS, Institute of Software, Chinese Academy of Sciences, Beijing,100190, China.
wwl@tca.iscas.ac.cn

Abstract. The *transparency order* (denoted by $\mathcal{TO}$) is a useful measure of the robustness of (n, m)-functions (cryptographic S-boxes as mappings from $GF(2)^n$ to $GF(2)^m$) to multi-bits Differential Power Analysis (D-PA). An improved version of transparency order (denoted by $\mathcal{RTO}$), based on the use of cross-correlation coefficients, was also introduced recently. For the first time, we resolve this open problem which (n, m)-functions reach the upper bound on $\mathcal{TO}$ for odd n (m is a power of 2). We also investigate the tightness of upper and lower bounds related to $\mathcal{RTO}$ and derive its relationship to main cryptographic characterizations of (n, m)-functions (such as nonlinearity, the sum-of-square indicator and algebraic immunity). Finally, concerning S-boxes of size 4×4, the distributions of $\mathcal{RTO}$ for all 302 balanced S-boxes (up to affine equivalence) and 16 equivalence classes of optimal S-boxes are given.

Keywords: (n, m)-functions · Transparency order · Nonlinearity · Auto-correlation · Cross-correlation.

1 Introduction

S-box is an important non-linear component of cryptographic algorithms. A careful selection of an S-box is required for ensuring cryptographic robustness of block (or stream) ciphers, at the same time aiming at efficient implementation.

In fact, most attacks on symmetric algorithms choose S-box as the target. For example, in side channel attacks, the secret key (used in the implementation of symmetric algorithms) can be recovered by analyzing the relationship between its leakages and the output of an S-box. For the first time, at CRYPTO 1999, Kocher et al. proposed differential power analysis (DPA) [5]. Then, the security of S-boxes against DPA was analyzed [1, 10]. At FSE 2005, the transparency order ($\mathcal{TO}$) based on the auto-correlation coefficients of (n, m)-functions was proposed by Prouff [10]. According to the definition of $\mathcal{TO}$, (n, m)-functions with smaller $\mathcal{TO}$ are more secure against DPA attacks. At INDOCRYPT 2005, Carlet obtained a lower bound of $\mathcal{TO}$ for highly non-linear (n, m)-functions. Besides, he also deduced a relationship between $\mathcal{TO}$ and the non-linearity for any (n, m)-function [1]. Later, Fan et al. proposed a fast computation technique for $\mathcal{TO}$ [4]. Then, Picek et al. proposed a genetic algorithm to find some Boolean functions with better $\mathcal{TO}$ values [9]. Mazumdar et al. also focused on the search of S-boxes with better $\mathcal{TO}$ values [7].

Recently, Chakraborty et al. proposed a revised definition of the transparency order (denoted by $\mathcal{RTO}$) based on the cross-correlation coefficients of (n, m)-functions (thus not only auto-correlation) in [3]. Consequently, cryptographically strong S-boxes, apart from satisfying standard cryptographic criteria such as high algebraic degree, high nonlinearity and good differential properties, also need to possess relatively large $\mathcal{RTO}$ to withstand DPA-like attacks. However, the analysis in [3] does not provide a thorough treatment regarding the properties of $\mathcal{RTO}$, thus no tight lower and upper bounds are given and its relation to other cryptographic criteria was not elaborated. A tight upper bound on $\mathcal{RTO}$ for Boolean functions was established in [13] and it was additionally shown that the lower bound directly depends on the nonlinearity. The latter result can be interpreted as a negative trade-off between nonlinearity and $\mathcal{RTO}$, stating that Boolean functions (as coordinate functions of an (n, m)-function or S-box) with high nonlinearity also have larger transparency order which is not a desirable feature in the context of DPA attacks. This also implies that the design of S-boxes satisfying all the cryptographic criteria including a low $\mathcal{RTO}$ becomes even a more demanding task.

So far, little has been done about addressing the problems related to identification of (n, m)-functions reaching the bounds on the (revised) transparency order and even less efforts have been made towards theoretical design of (n, m)-functions having relatively good transparency order and at the same time satisfying other cryptographic criteria. In this article, we address some open problems related to both definitions of transparency order. Firstly, whereas some instances of (n, m)-functions reaching the upper bound for even n were given in [10], we consider the problem of specifying (n, m)-functions achieving the upper bound on $\mathcal{TO}$ (thus the worst possible case concerning DPA) which was left open in [10] for odd n. We explicitly specify those classes of (n, m)-functions having the maximum possible $\mathcal{TO}$ when m is a power of 2. Secondly, to further elaborate on the design of robust (n, m)-functions with respect to the $\mathcal{RTO}$ indicator [3], we establish some important connections between $\mathcal{RTO}$ and other cryptograph-

ic properties such as the *sum-of-square indicator*, *algebraic immunity* (AI), and *nonlinearity* of the coordinate functions of (n, m)-functions. In particular, it is shown that not only the nonlinearity impacts $\mathcal{RTO}$ but also the sum-of-square indicator (as expected) has a direct influence on the resistance to DPA attacks.

Furthermore, the established connection between the algebraic immunity and transparency order essentially indicates (along with other trade-offs) that the design of cryptographically secure (n, m)-functions is hard to achieve if the protection against DPA attacks is taken into account. In this direction, it would be interesting to establish a similar connection between differential properties of (n, m)-functions and $\mathcal{RTO}$.

Finally, concerning the upper and lower bounds on $\mathcal{RTO}$, for the first time their tightness has been confirmed through explicit examples. Moreover, we have also computed the transparency order for all S-boxes of size 4×4 (up to affine equivalence) which gives a complete insight in their properties related to $\mathcal{RTO}$.

This paper is organized as follows. In Section 2, some notations and definitions related to Boolean functions are given. Besides, we recall two different notions of transparency order. In Section 3, in connection to the transparency order introduced by Prouff [10], we provide certain classes of (n, m)-functions reaching the upper bound of $\mathcal{TO}$. We also specify several connections between the recently introduced $\mathcal{RTO}$ indicator and some main cryptographic parameters, and additionally derive a tight lower and upper bound on $\mathcal{RTO}$. In Section 4, we provide distributions of the transparency order for all S-boxes of size 4×4 (up to affine equivalence). Finally, some concluding remarks are given in Section 5.

2 Preliminaries

In this section, we give some definitions of Boolean functions and the transparency order, and introduce some indicators for Boolean functions.

2.1 Definition of Boolean functions

The set of n-variable Boolean functions is denoted by $\mathbb{B}_n$, where any $f \in \mathbb{B}_n$ is simply a mapping $f : \mathbb{F}_2^n \to \mathbb{F}_2$. We denote by $\oplus$ the addition modulo two performed in $\mathbb{F}_2$ and the vector space $\mathbb{F}_2^n$. Every Boolean function $f \in \mathbb{B}_n$ admits a unique representation called the algebraic normal form (ANF) which is a multivariate polynomial over $\mathbb{F}_2$:

$$f(x_1, \ldots, x_n) = a_0 \oplus \bigoplus_{1 \le i \le n} a_i x_i \oplus \bigoplus_{1 \le i < j \le n} a_{i,j} x_i x_j \oplus \cdots \oplus a_{1,\ldots,n} x_1 x_2 \cdots x_n,$$

where the coefficients $a_0, a_i, a_{i,j}, \cdots, a_{1,\ldots,n} \in \mathbb{F}_2$. The algebraic degree, $deg(f)$, is the largest length of the monomial(s) with non-zero coefficients.

Let $supp(f) = \{(x_1, \ldots, x_n) \in \mathbb{F}_2^n \mid f(x_1, \ldots, x_n) = 1\}$ and $wt(f)$ be the Hamming weight of f, then $wt(f) = |supp(f)|$. Furthermore, if $wt(f) = 2^{n-1}$

for any $f \in \mathbb{B}_n$, then f is said to be balanced. We denote by $\mathbb{A}_n$ the set of affine functions, that is, $deg(f) \leq 1$ in this set.

In this paper, let $\mathbf{0}^n = \{\underbrace{0, \ldots, 0}_{n}\}$ and $\mathbf{1}^n = \{\underbrace{1, \ldots, 1}_{n}\}$ denote the all-zero and all-one vectors, respectively.

2.2 Some indicators for Boolean functions

Nonlinearity is an important indicator to measure the linearity of Boolean functions. Boolean functions with higher nonlinearity are more resistant to linear attacks.

Definition 1. *Let $f \in \mathbb{B}_n$. The nonlinearity of f can be computed using*

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

where $\mathcal{F}(f \oplus \varphi_\alpha)$ is the Walsh spectral value of f at point $\alpha \in \mathbb{F}_2^n$ computed as:

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

where $\varphi_\alpha(x) = \alpha \cdot x = \alpha_1 x_1 \oplus \cdots \oplus \alpha_n x_n$.

Based on the nonlinearity of $f \in \mathbb{B}_n$ and the well-known Parseval's equation, we know that f is a *bent* function [11] if $N_f = 2^{n-1} - 2^{n/2-1}$ for even n.

The cross-correlation and the auto-correlation functions play an important role in this paper. For any $f, g \in \mathbb{B}_n$, the cross-correlation function is defined as

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

If $f = g$ in the above formula, then the auto-correlation function of f is given by $\triangle_f(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus \alpha)}, \alpha \in \mathbb{F}_2^n$.

In order to measure the correlation between two Boolean functions, we recall the definition of perfectly uncorrelated functions. Two Boolean functions $f, g \in \mathbb{B}_n$ are said to be perfectly uncorrelated if $\triangle_{f,g}(\alpha) = 0$, for any $\alpha \in \mathbb{F}_2^n$. Sarkar et al. [12] proved that $\mathcal{F}(f \oplus \varphi_\alpha)\mathcal{F}(g \oplus \varphi_\alpha) = 0$ for any $\alpha \in \mathbb{F}_2^n$ if and only if f and g are perfectly uncorrelated. Later, Pasalic et al. [8] proved that f and g are disjoint spectra functions (meaning that $\mathcal{F}(f \oplus \varphi_\alpha) = 0$ implies that $\mathcal{F}(g \oplus \varphi_\alpha) \neq 0$ or vice versa) if and only if f and g are perfectly uncorrelated. In order to better prove some conclusions in this paper, we give the definition of *almost perfectly uncorrelated* functions.

Definition 2. *Let $f, g \in \mathbb{B}_n$. f and g are almost perfectly uncorrelated, if $\triangle_{f,g}(\alpha) = 0$ for any $\alpha \in \mathbb{F}_2^{n*}$, where $\mathbb{F}_2^{n*} = \mathbb{F}_2^n \setminus \mathbf{0^n}$.*

Definition 2 implies that f and g are almost perfectly uncorrelated if f and g are perfectly uncorrelated.

In order to characterize the so-called global avalanche property, Zhang et al. [14] introduced an indicator based on the auto-correlation function of a Boolean function.

Definition 3. *Let $f \in \mathbb{B}_n$. The global avalanche characteristics (GAC) of f is given by:*

$$\sigma_f = \sum_{\alpha \in \mathbb{F}_2^n} [\triangle_f(\alpha)]^2, \qquad \triangle_f = \max_{\alpha \in \mathbb{F}_2^n, \alpha \neq \mathbf{0}^n} \mid \triangle_f(\alpha) \mid .$$

In 2010, Zhou et al. [16] generalized Definition 3, and presented the notions of the *absolute indicator* and the *sum-of-squares indicator* (defined below respectively) based on the cross-correlation function for two Boolean functions $f, g \in \mathbb{B}_n$:

$$\triangle_{f,g} = \max_{\alpha \in \mathbb{F}_2^n, wt(\alpha) \neq 0} \mid \triangle_{f,g}(\alpha) \mid, \qquad \sigma_{f,g} = \sum_{\alpha \in \mathbb{F}_2^n} [\triangle_{f,g}(\alpha)]^2.$$

2.3 Definition of (n, m)-functions and the transparency order

In this paper, we study some properties of the transparent order properties for (n, m)-functions, therefore we first give the definition of (n, m)-functions.

Let $f_i \in \mathbb{B}_n (i = 1, 2, \ldots, m)$. If $F = (f_1, \ldots, f_m) : \mathbb{F}_2^n \to \mathbb{F}_2^m$, then F is called an (n, m)-function. An (n, m)-function F is balanced if and only if its *component functions* are balanced, meaning that for every nonzero $v \in \mathbb{F}_2^m$ the Boolean function $v \cdot F$ is balanced. Thus, the balanced (n, n)-functions are the permutations on $\mathbb{F}_2^n$.

Based on the auto-correlation and cross-correlation functions and the definition of (n, m)-functions, Prouff [10] introduced the concept of transparency order.

Definition 4. *[10] Let $F = (f_1, \ldots, f_m)$ be an (n, m)-function. The transparency order is defined by:*

$$\mathcal{TO}(F) = \max_{\beta \in \mathbb{F}_2^m} \{ \mid m - 2wt(\beta) \mid - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \big| \sum_{i=1}^{m} (-1)^{\beta_i} \triangle_{f_i}(a) \big| \}. \qquad (1)$$

Later, Chakraborty et al. [3] revised this definition by using cross-correlation properties, which then reflects DPA attacks in the Hamming weight model in a more transparent manner. In order to be consistent with (n, m)-functions in Definition 4 and to address the properties of (n, m)-functions in general, we extend the original definition of balanced (n, m)-functions to any (n, m)-functions.

Definition 5. *[3] Let $F = (f_1, \ldots, f_m)$ be an (n, m)-function. The transparency order of F is defined by:*

$$\mathcal{RTO}(F) = \max_{\beta \in \mathbb{F}_2^m} \{ m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \sum_{j=1}^{m} \big| \sum_{i=1}^{m} (-1)^{\beta_i \oplus \beta_j} \triangle_{f_i, f_j}(a) \big| \}. \qquad (2)$$

The above expression can be further manipulated to give

$$\mathcal{RTO}(F) = \max_{\beta \in \mathbb{F}_2^m} \{m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \sum_{j=1}^{m} \big| \sum_{i=1}^{m} \triangle_{f_i \oplus \beta_i, f_j \oplus \beta_j}(a) \big| \}.$$

The following quantities, for a given $\beta \in \mathbb{F}_2^m$, will be proved useful in the sequel:

$$\Gamma_F^\beta = m - \nu_{F,\beta}. \tag{3}$$

$$\nu_{F,\beta} = \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \sum_{j=1}^{m} \mid \sum_{i=1}^{m} \triangle_{f_i \oplus \beta_i, f_j \oplus \beta_j}(a) \mid . \tag{4}$$

3 Cryptographic properties of $\mathcal{RTO}$

In this section, we give the existence of (n, m)-functions reaching the upper bound m on $\mathcal{TO}$, then we provide tight upper and lower bounds on $\mathcal{RTO}$ and deduce some cryptographic properties of $\mathcal{RTO}$.

3.1 The existence of (n, m)-functions reaching the upper bound m on $\mathcal{TO}$

For the standard definition of transparency order given by Definition 4, Prouff [10] showed that the maximum value of $\mathcal{TO}$ of an (n, m)-function F equals to m when n is even, and it can be easily achieved if every coordinate function is a bent function. On the other hand, it was left as an open problem to specify a class of vectorial (n, m)-functions satisfying $\mathcal{TO}(F) = m$ when n is odd. The solution to this problem is given below, so that the existence of (n, m)-functions or S-boxes (for m being a power of two), regardless the parity of n, having the largest possible transparency order (the worst case regarding the resistance to DPA) is now asserted.

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

1) *If n is even, then defining f_i to be a bent function for all $1 \le i \le m$ implies that $\mathcal{TO}(F) = m$.*

2) *For $n \ge 4$ and $m = 2^k$, where $n \ge m$ and $k \ge 2$, let $g \in \mathbb{B}_{n-k}$ be a bent function (thus $n - k$ is even). Define $F = (f_1, \ldots, f_m)$ through its coordinate functions given by,*

$$f_i(x, y) = g(x) \oplus \omega_i \cdot y, \qquad x \in \mathbb{F}_2^{n-k}, y \in \mathbb{F}_2^k,$$

where $\omega_i \in \mathbb{F}_2^k$ for $1 \le i \le m = 2^k$ and $\omega_i \ne \omega_j$ when $i \ne j$. Then, $\mathcal{TO}(F) = m$.

Proof. 1) This result is proved in [10].
2) For any $\omega_i, \gamma \in \mathbb{F}_2^k$ and $\alpha \in \mathbb{F}_2^{n-k}$, we compute the auto-correlation of f_i as:

$$\triangle_{f_i}(\alpha, \gamma) = \sum_{x \in \mathbb{F}_2^{n-k}, y \in \mathbb{F}_2^k} (-1)^{f_i(x,y) \oplus f_i(x \oplus \alpha, y \oplus \gamma)}$$

$$
\begin{aligned}
&= \sum_{x\in\mathbb{F}_2^{n-k}, y\in\mathbb{F}_2^k} (-1)^{g(x)\oplus\omega_i\cdot y\oplus g(x\oplus\alpha)\oplus\omega_i\cdot(y\oplus\gamma)} \\
&= \sum_{y\in\mathbb{F}_2^k} (-1)^{\omega_i\cdot y\oplus\omega_i\cdot(y\oplus\gamma)} \sum_{x\in\mathbb{F}_2^{n-k}} (-1)^{g(x)\oplus g(x\oplus\alpha)} \\
&= 2^k(-1)^{\omega_i\cdot\gamma} \sum_{x\in\mathbb{F}_2^{n-k}} (-1)^{g(x)\oplus g(x\oplus\alpha)} \\
&= \begin{cases} 2^n(-1)^{\omega_i\cdot\gamma}, & \alpha = \mathbf{0}^{n-k}; \\ 0, & \alpha \neq \mathbf{0}^{n-k}. \end{cases}
\end{aligned}
$$

For $\beta = (\beta_1, \ldots, \beta_m) \in \mathbb{F}_2^m$, we can express $\mathcal{TO}(F)$ as:

$$
\begin{aligned}
\mathcal{TO}(F) &= \max_{\beta\in\mathbb{F}_2^m}\{\mid m - 2wt(\beta) \mid - \frac{1}{2^{2n}-2^n} \sum_{a=(\alpha,\gamma)\in\mathbb{F}_2^{n*}} \big|\sum_{i=1}^{m} \triangle_{f_i\oplus\beta_i}(a)\big|\} \\
&= \max_{\beta\in\mathbb{F}_2^m}\{\big|m - 2wt(\beta) \mid - \frac{2^n}{2^{2n}-2^n} \sum_{\gamma\in\mathbb{F}_2^{k*}} \mid (-1)^{\omega_1\cdot\gamma\oplus\beta_1} + \cdots + \\
&\quad (-1)^{\omega_m\cdot\gamma\oplus\beta_m}\big|\} \\
&= \max_{\beta\in\mathbb{F}_2^m}\{\big|m - 2wt(\beta) \mid - \frac{2^n}{2^{2n}-2^n} \sum_{\gamma\in\mathbb{F}_2^{k*}} \mid \sum_{i=1}^{m}(-1)^{\omega_i\cdot\gamma\oplus\beta_i}\big|\}. \qquad (5)
\end{aligned}
$$

When $wt(\beta) = m$ or $wt(\beta) = 0$, then

$$
\mathcal{TO}(F) = \max_{\beta\in\mathbb{F}_2^m}\{m - \frac{2^n}{2^{2n}-2^n} \sum_{\gamma\in\mathbb{F}_2^{k*}} \mid \sum_{i=1}^{m}(-1)^{\omega_i\cdot\gamma} \mid\}.
$$

Noting that $\sum_{i=1}^{m}(-1)^{\omega_i\cdot\gamma} = 0$, for $\gamma \in \mathbb{F}_2^{k*}$, we obtain

$$
\mathcal{TO}(F) = \max_{\beta\in\mathbb{F}_2^m}\{m - 0\} = m. \blacksquare
$$

Example 1 *Let $F = (f_1, \ldots, f_4)$ be an $(n, 4)$ function whose coordinate functions are defined as:*

$$
\begin{gathered}
f_1(x, y_1, y_2) = g(x) \oplus y_1 \oplus y_2,\ \ f_2(x, y_1, y_2) = g(x) \oplus y_1, \\
f_3(x, y_1, y_2) = g(x) \oplus y_2,\ \ f_4(x, y_1, y_2) = g(x),
\end{gathered}
$$

where g is a bent $(n-2)$-variable function and n is even. Then $\mathcal{TO}(F) = 4$, which can be confirmed with help of the auto-correlation coefficients of f_i given in Table 1, where $\gamma \in \mathbb{F}_2^{n-2}$ and $\gamma_1, \gamma_2 \in \mathbb{F}_2$.

Then using (5) and the auto-correlation values in Table 1, it can be easily verified that for $\beta = (1, 1, 1, 1)$ or $\beta = (0, 0, 0, 0)$, we have $\mathcal{TO}(F) = \max_{\beta\in\mathbb{F}_2^4}\{\mid 4 - 2wt(\beta) \mid -0\} = 4$.

Table 1. Auto-correlation values of the coordinate functions of F in Example 1

$\alpha = (\gamma, \gamma_1, \gamma_2)$	$(\mathbf{0}^{n-2}, 0, 0)$	$(\mathbf{0}^{n-2}, 0, 1)$	$(\mathbf{0}^{n-2}, 1, 0)$	$(\mathbf{0}^{n-2}, 1, 1)$	else
$\triangle_{f_1}(\alpha)$	2^n	-2^n	-2^n	2^n	0
$\triangle_{f_2}(\alpha)$	2^n	2^n	-2^n	-2^n	0
$\triangle_{f_3}(\alpha)$	2^n	-2^n	2^n	-2^n	0
$\triangle_{f_4}(\alpha)$	2^n	2^n	2^n	2^n	0

A similar analysis can be performed for odd n, defining for simplicity two coordinate functions for $(x, y) \in \mathbb{F}_2^{n-1} \times \mathbb{F}_2$:

$$f_1(x, y) = g(x) \oplus y, \;\; f_2(x, y) = g(x),$$

where $g(x)$ is a bent function so that $n - 1$ is even. Again, $F = (f_1, f_2)$ reaches the upper bound on $\mathcal{TO}$, thus $\mathcal{TO}(F) = 2$.

Example 1 of Theorem 1 illustrates the specification of (n, m)-function achieving the upper bound on $\mathcal{TO}$.

Remark 1 *There are several observations worth of noticing in connection to Theorem 1. In the first place, none of these $f_i(x, y) = g(x) + \omega_i y$ is a bent function and therefore this method differs substantially from the result in [10]. It can be easily verified that f_i and f_j are disjoint spectra functions. Furthermore, when n is odd (which necessarily implies that k is odd) the result of Theorem 1 essentially solves the open problem in [10] of finding (n, m) functions reaching the upper bound on $\mathcal{TO}$ if m is a power of 2. The nonlinearity of the coordinate functions given by $2^{n-1} - \frac{1}{2} \times 2^{\frac{n-k}{2}} 2^k = 2^{n-1} - 2^{\frac{n+k}{2}-1}$ is rather high which confirms its negative impact on $\mathcal{TO}$.*

In the following, we perform a detailed theoretical analysis of the revised transparency order $\mathcal{RTO}$ [3]. We first provide sharp and general lower and upper bound of $\mathcal{RTO}$ for a class of almost perfectly uncorrelated functions and specify the instances of S-boxes achieving these bounds. In addition, we derive some useful connections that relate $\mathcal{RTO}$ to other cryptographic notions such as nonlinearity, algebraic immunity and cross-correlation coefficients. A general conclusion is that attaining a low $\mathcal{RTO}$ indicator (thus offering a higher resistance to side-channel cryptanalysis) induces a certain worsening of other cryptographic criteria. Therefore, providing an optimal design of cryptographic S-boxes that possess sufficient robustness to both standard cryptanalytic attacks as well as to side-channel cryptanalysis appears to be a quite demanding task.

3.2 The upper and lower bounds on $\mathcal{RTO}(F)$

In this section, we give the upper and lower bounds on $\mathcal{RTO}$ by using almost perfectly uncorrelated functions. Based on Definition 5 of the transparency order, a lower bound on $\mathcal{RTO}$ was derived in [3] in terms of the Walsh spectrum of

the coordinate functions of (n, m)-functions. Before we provide a tight lower and upper bound on $\mathcal{RTO}$, employing the concept of almost perfectly uncorrelated functions, we give some simple preparatory results.

Lemma 1. *Let $F = (f_1, \ldots, f_m)$ be a balanced (n, m)-function, where $x \in \mathbb{F}_2^n$. Then, $F \oplus \beta = (f_1 \oplus \beta_1, \ldots, f_m \oplus \beta_m)$ is also a balanced (n, m)-function for any $\beta = (\beta_1, \ldots, \beta_m) \in \mathbb{F}_2^m$.*

Proof. The fact that $F = (f_1, \ldots, f_m)$ is a balanced vectorial Boolean function, implies that $v \cdot F$ is a balanced Boolean function for any $v \in \mathbb{F}_2^{n*}$ and the result follows. ■

Lemma 2. *Let $F = (f_1, \ldots, f_m)$ be a balanced (n, m)-function. Then, f_i and f_j are almost perfectly (or perfectly) uncorrelated for any $1 \leq i < j \leq m$ if and only if $f_i \oplus \beta_i$ and $f_j \oplus \beta_j$ are (almost) perfectly uncorrelated for any $1 \leq i < j \leq m$, where $\beta = (\beta_1, \ldots, \beta_m) \in \mathbb{F}_2^m$.*

Proof. For any $\beta = (\beta_1, \ldots, \beta_m) \in \mathbb{F}_2^m$ and $\alpha \in \mathbb{F}_2^n$ we have

$$\begin{aligned}
\triangle_{f_i \oplus \beta_i, f_j \oplus \beta_j}(\alpha) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f_i(x) \oplus \beta_i \oplus f_j(x \oplus \alpha) \oplus \beta_j} \\
&= (-1)^{\beta_i \oplus \beta_j} \sum_{x \in \mathbb{F}_2^n} (-1)^{f_i(x) \oplus f_j(x \oplus \alpha)} \\
&= (-1)^{\beta_i \oplus \beta_j} \triangle_{f_i, f_j}(\alpha).
\end{aligned}$$

Thus, $f_i(x) \oplus \beta_i$ and $f_j(x) \oplus \beta_j$ are (almost) perfectly uncorrelated if and only if $f_i(x)$ and $f_j(x)$ are (almost) perfectly uncorrelated for any $1 \leq i < j \leq m$, $\alpha \in \mathbb{F}_2^n$ and $\beta \in \mathbb{F}_2^n$. ■

Theorem 2. *Let $F = (f_1, \ldots, f_m)$ be an (n, m)-function, $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. If f_i and f_j are almost perfectly uncorrelated functions for $1 \leq i \neq j \leq m$, then*

$$0 \leq \mathcal{RTO}(F) \leq m.$$

Especially, $\mathcal{RTO}(F) = m$ if and only if $\triangle_{f_i}(\alpha) = 0$ for any $\alpha \in \mathbb{F}_2^{n*}$ and $1 \leq i \leq m$. Also, $\mathcal{RTO}(F) = 0$ if and only if $\mid \triangle_{f_i}(\alpha) \mid = 2^n$ for any $\alpha \in \mathbb{F}_2^{n*}$ and $1 \leq i \leq m$.

Proof. Since f_i and f_j are almost perfectly uncorrelated for any $1 \leq i \neq j \leq m$, we have $\triangle_{f_i, f_j}(a) = 0$ for any $a \in \mathbb{F}_2^{n*}$. Then,

$$\begin{aligned}
\Gamma_F^\beta &= m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \sum_{j=1}^{m} \Big| \sum_{i=1}^{m} \triangle_{f_i \oplus \beta_i, f_j \oplus \beta_j}(a) \Big| \\
&= m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \sum_{j=1}^{m} \big| \triangle_{f_1 \oplus \beta_1, f_j \oplus \beta_j}(a) + \cdots \\
&\quad + \triangle_{f_j \oplus \beta_j, f_j \oplus \beta_j}(a) + \cdots + \triangle_{f_m \oplus \beta_m, f_j \oplus \beta_j}(a) \big|
\end{aligned}$$

$$= m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \sum_{j=1}^{m} \left| \triangle_{f_j \oplus \beta_j, f_j \oplus \beta_j}(a) \right|$$

$$= m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \sum_{j=1}^{m} \left| \triangle_{f_j \oplus \beta_j}(a) \right|$$

For any $f_j(x) \oplus \beta_j$, with $1 \leq j \leq m$, we know that $0 \leq | \triangle_{f_j \oplus \beta_j}(a) | \leq 2^n$. Thus, $0 \leq \Gamma_F^{\beta} \leq m$, that is, $0 \leq \mathcal{RTO}(F) \leq m$.

In particular, we have $\mathcal{RTO}(F) = m$ if and only if $| \triangle_{f_j \oplus \beta_j}(a) | = 0$, for any $\alpha \in \mathbb{F}_2^{n*}$ and $1 \leq i \leq m$. Similarly, $\mathcal{RTO}(F) = 0$ if and only if $| \triangle_{f_i}(\alpha) | = 2^n$, for any $\alpha \in \mathbb{F}_2^n \setminus \mathbf{0}^n$ and $1 \leq i \leq m$. ■

Example 2 *Let $F = (f_1, f_2)$ be a $(4, 2)$-function whose coordinate functions are bent and given by:*

$$f_1(x) = x_1x_2 \oplus x_3x_4, \;\; f_2(x) = x_1x_2 \oplus x_3x_4 \oplus 1.$$

We deduce that $\triangle_{f_i}(a) = 0$ and $\triangle_{f_i, f_j}(a) = 0$ for any $a \in \mathbb{F}_2^{n*}$. We have

$$\Gamma_F^{\beta} = m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \sum_{j=1}^{m} | \sum_{i=1}^{m} \triangle_{f_i \oplus \beta_i, f_j \oplus \beta_j}(a) | = m - 0 = m,$$

so that $\mathcal{RTO}(F) = m = 2$.

Example 3 *Let $F = (f_1, \ldots, f_4)$ be an $(8, 4)$-function, thus $F : \mathbb{F}_2^8 \to \mathbb{F}_2^4$, with its coordinate (linear) functions specified as:*

$$f_1(x) = x_1 \oplus x_2, \quad f_2(x) = x_3 \oplus x_4, \quad f_3(x) = x_5 \oplus x_6, \quad f_4(x) = x_7 \oplus x_8.$$

It is easily verified that $| \triangle_{f_i}(a) | = 2^n$ and $\triangle_{f_i, f_j}(a) = 0$ for any $a \in \mathbb{F}_2^{n*}$, where $n = 8$. Then,

$$\Gamma_F^{\beta} = m - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \sum_{j=1}^{m} | \sum_{i=1}^{m} \triangle_{f_i \oplus \beta_i, f_j \oplus \beta_j}(a) | = m - \frac{m2^n(2^n - 1)}{2^{2n} - 2^n} = 0,$$

implying that $\mathcal{RTO}(F) = 0$.

Example 2 and Example 3 illustrate the specification of (n, m)-function achieving the upper bound on $\mathcal{RTO}$ in Theorem 2, respectively.

Remark 2 *If we take f to be bent and let $F = (f, 1 \oplus f)$, we deduce that $\mathcal{RTO}(F) = 2$, thus reaching the upper bound on $\mathcal{RTO}$ of $(n, 2)$-functions when n is even. This confirms that using bent functions corresponds to the worst case with respect to DPA, whereas linear S-boxes offer the highest resistance to DPA.*

3.3 Relating $\mathcal{RTO}$ to the absolute cross-correlation indicator

An upper bound on $\mathcal{RTO}$ can be also stated in terms of the absolute indicator (computed at zero for particular shifts of input functions) which is then useful for two purposes. In the first place, employing the fact that for certain classes of Boolean functions the values of this indicator are known, one can easily specify certain S-boxes reaching the upper bound. Moreover, a similar reasoning allows us to also specify S-boxes (of certain size) whose transparency order is provably smaller than the upper bound.

Lemma 3. *[16] For two Boolean functions $f, g \in \mathbb{B}_n$, the following holds:*

$$\sum_{\alpha \in \mathbb{F}_2^n} \triangle_{f,g}(\alpha) = (2^n - 2wt(f))(2^n - 2wt(g)).$$

Using Lemma 3, for (n, m)-functions, one can deduce an upper bound on $\mathcal{RTO}(F)$ that depends on $\triangle_{f_i \oplus \beta_i, f_j \oplus \beta_j}(\mathbf{0^n})$.

Theorem 3. *Let $F = (f_1, \ldots, f_m)$ be an (n, m)- function and $wt(f_i) = 2^{n-1} (1 \leq i \leq m)$. Then*

$$\mathcal{RTO}(F) \leq m - \frac{1}{2^{2n} - 2^n} \Big| \sum_{j=1}^{m} \sum_{i=1}^{m} [\triangle_{f_i \oplus \beta_i, f_j \oplus \beta_j}(\mathbf{0^n})] \Big|,$$

where $\beta = (\beta_1, \ldots, \beta_m) \in \mathbb{F}_2^m$.

Proof. Using the inequality $\sum\limits_{i=1}^{m} \mid a_i \mid \geq \mid \sum\limits_{i=1}^{m} a_i \mid$ for any $a_i \in \mathbb{R}$, we have

$$\begin{aligned}
\nu_{F,\beta} &= \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \sum_{j=1}^{m} \Big| \sum_{i=1}^{m} \triangle_{f_i \oplus \beta_i, f_j \oplus \beta_j}(a) \Big| \\
&\geq \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \Big| \sum_{j=1}^{m} \sum_{i=1}^{m} \triangle_{f_i \oplus \beta_i, f_j \oplus \beta_j}(a) \Big| \\
&\geq \frac{1}{2^{2n} - 2^n} \Big| \sum_{a \in \mathbb{F}_2^{n*}} \sum_{j=1}^{m} \sum_{i=1}^{m} \triangle_{f_i \oplus \beta_i, f_j \oplus \beta_j}(a) \Big| \\
&= \frac{1}{2^{2n} - 2^n} \Big| \sum_{j=1}^{m} \sum_{i=1}^{m} \sum_{a \in \mathbb{F}_2^{n*}} [\triangle_{f_i \oplus \beta_i, f_j \oplus \beta_j}(a)] \Big| \\
&= \frac{1}{2^{2n} - 2^n} \Big| \sum_{j=1}^{m} \sum_{i=1}^{m} [\sum_{a \in \mathbb{F}_2^{n}} [\triangle_{f_i \oplus \beta_i, f_j \oplus \beta_j}(a)] - \triangle_{f_i \oplus \beta_i, f_j \oplus \beta_j}(\mathbf{0}^n)] \Big|.
\end{aligned}$$

Since f_i is a balanced function for $1 \leq i \leq m$, by Lemma 3, we have

$$\nu_{F,\beta} \geq \frac{1}{2^{2n} - 2^n} \Big| \sum_{j=1}^{m} \sum_{i=1}^{m} [[2^n - 2wt(f_i \oplus \beta_i)][2^n - 2wt(f_j \oplus \beta_j)] -$$

$$\begin{aligned}
&\triangle_{f_i\oplus\beta_i,f_j\oplus\beta_j}(\mathbf{0}^n)]\big| \\
&= \frac{1}{2^{2n}-2^n}\big|\sum_{j=1}^{m}\sum_{i=1}^{m}[-\triangle_{f_i\oplus\beta_i,f_j\oplus\beta_j}(\mathbf{0}^n)]\big| \\
&= \frac{1}{2^{2n}-2^n}\big|\sum_{j=1}^{m}\sum_{i=1}^{m}[\triangle_{f_i\oplus\beta_i,f_j\oplus\beta_j}(\mathbf{0}^n)]\big|,
\end{aligned}$$

which proves the result. ■

If f_i and f_j are perfectly uncorrelated functions for $1 \le i \ne j \le m$, then $\triangle_{f_i\oplus\beta_i,f_j\oplus\beta_j}(a) = 0$ for any $1 \le i \ne j \le m$. From the proof of Theorem 3, we have

$$\begin{aligned}
\nu_{F,\beta} &\ge \frac{1}{2^{2n}-2^n}\big|\sum_{j=1}^{m}\sum_{i=1}^{m}[\triangle_{f_i\oplus\beta_i,f_j\oplus\beta_j}(\mathbf{0}^n)]\big| \\
&= \frac{1}{2^{2n}-2^n}\big|\sum_{i=1}^{m}[\triangle_{f_i\oplus\beta_i,f_i\oplus\beta_i}(\mathbf{0}^n)]\ \big| \\
&= \frac{m\times 2^n}{2^{2n}-2^n} \\
&= \frac{m}{2^n-1}.
\end{aligned}$$

Corollary 1. *Let $F = (f_1, \ldots, f_m)$ be an (n, m)-function and $wt(f_i) = 2^{n-1}(1 \le i \le m)$. If the coordinate functions f_i and f_j are perfectly uncorrelated for $1 \le i \ne j \le m$, then*

$$\mathcal{RTO}(F) \le m - \frac{m}{2^n-1}.$$

The following example illustrate the possibility of specifying (n, m)-functions whose transparency order $\mathcal{RTO}$ is smaller than the upper bound.

Example 4 *Let $F = (f_1, f_2)$ be an $(n, 2)$-function, and define f_i as:*

$$f_1(x, y_1, y_2) = g(x) \oplus y_1 \oplus y_2, \quad f_2(x, y_1, y_2) = g(x) \oplus y_1,$$

where n is even, $x \in \mathbb{F}_2^{n-2}, y_1, y_2 \in \mathbb{F}_2$, $g \in \mathbb{B}_{n-2}$ is a bent function. Then, $\mathcal{TO}(F) = 2 - \frac{6}{2^n-1}$. The distribution of auto-correlation coefficients of f_i are given in Table 2.

Table 2. Distribution of auto-correlation and cross-correlation functions of $F(x, y_1, y_2)$

$\alpha = (\gamma, \gamma_1, \gamma_2)$	$(\mathbf{0}^{n-2}, 0, 0)$	$(\mathbf{0}^{n-2}, 0, 1)$	$(\mathbf{0}^{n-2}, 1, 0)$	$(\mathbf{0}^{n-2}, 1, 1)$	else
$\triangle_{f_1}(\alpha)$	2^n	-2^n	-2^n	2^n	0
$\triangle_{f_2}(\alpha)$	2^n	2^n	-2^n	-2^n	0
$\triangle_{f_1,f_2}(\alpha)$	0	0	0	0	0

Using Table 2, we obtain

$$\begin{aligned}
\Gamma_F^{\beta} &= 2 - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \sum_{j=1}^{2} \Big| \sum_{i=1}^{2} \triangle_{f_i \oplus \beta_i, f_j \oplus \beta_j}(a) \Big| \\
&= 2 - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} \sum_{j=1}^{2} \big| \triangle_{f_1 \oplus \beta_1, f_j \oplus \beta_j}(a) + \triangle_{f_2 \oplus \beta_2, f_j \oplus \beta_j}(a) \big| \\
&= 2 - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} [\big| \triangle_{f_1 \oplus \beta_1, f_1 \oplus \beta_1}(a) + \triangle_{f_2 \oplus \beta_2, f_1 \oplus \beta_1}(a) \big| \\
&\quad + \big| \triangle_{f_1 \oplus \beta_1, f_2 \oplus \beta_2}(a) + \triangle_{f_2 \oplus \beta_2, f_2 \oplus \beta_2}(a) \big|] \\
&= 2 - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} [\big| \triangle_{f_1 \oplus \beta_1, f_1 \oplus \beta_1}(a) \big| + \big| \triangle_{f_2 \oplus \beta_2, f_2 \oplus \beta_2}(a) \big|] \\
&= 2 - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbb{F}_2^{n*}} [\big| (-1)^{\beta_1 \oplus \beta_1} \triangle_{f_1, f_1}(a) \mid + \big| (-1)^{\beta_2 \oplus \beta_2} \triangle_{f_2, f_2}(a) \big|] \\
&= 2 - \frac{6 \times 2^n}{2^{2n} - 2^n} \\
&= 2 - \frac{6}{2^n - 1}.
\end{aligned}$$

Thus, $\mathcal{RTO}(F) = 2 - \frac{6}{2^n - 1} < 2 - \frac{2}{2^n - 1}$*, where the right-hand side value is the bound in Theorem 3.*

On the other hand, again using bent functions in the background, the derived disjoint spectra Boolean functions easily give rise to S-boxes reaching the upper bound of Corollary 1 (see Example 5).

Example 5 *Let n be an odd and $F = (f_1, f_2)$ be an $(n, 2)$-function with f_i given by $x \in \mathbb{F}_2^{n-1}$, $y \in \mathbb{F}_2$. If $F(x, y)$ is expressed as:*

$$f_1(x, y) = g(x) \oplus y, \quad f_2(x, y) = g(x), \quad (x, y) \in \mathbb{F}_2^{n-1} \times \mathbb{F}_2,$$

where $g \in \mathbb{B}_{n-1}$ is a bent function. Then, based on the fact that f_1 and f_2 are disjoint spectra functions (see e.g. [8]), it can be easily verified that $\mathcal{RTO}(F) = 2 - \frac{2}{2^n - 1}$.

3.4 The relationships between $\mathcal{RTO}$ and other cryptographic properties

To design robust S-boxes for cryptographic applications (referring mainly to their use in block ciphers), not only the transparency order should be moderately low but also the considered S-box should satisfy other cryptographic criteria such as good differential properties, low sum-of-square indicator, high nonlinearity, and high algebraic immunity and degree. Thus, the relationships between $\mathcal{RTO}$ and other cryptographic criteria is quite important. In the first place, the bounds on

$\mathcal{RTO}$ that depend on these quantities might give us a useful insight whether it is possible at all to design cryptographically robust S-boxes unifying all the relevant criteria.

The following result describes the relationship between $\mathcal{RTO}$ and the sum-of-square indicator.

Theorem 4. *Let $F = (f_1, \ldots, f_m)$ be a balanced (n, m)- function. If f_i and f_j are not almost perfectly uncorrelated for $1 \leq i \neq j \leq m$, then*

$$\mathcal{RTO}(F) \geq m - \frac{1}{2^n}\sqrt{\frac{m}{2^n-1}}\sum_{j=1}^{m}\left[\sum_{i=1}^{m}\sqrt{\sigma_{f_i}\sigma_{f_j}}\right]^{1/2}.$$

Proof. By using the Cauchy's inequality, for $\beta = (\beta_1, \cdots, \beta_m) \in \mathbb{F}_2^m$ we have

$$\begin{aligned}
\sum_{a\in\mathbb{F}_2^{n*}}\Big|\sum_{i=1}^{m}\triangle_{f_i\oplus\beta_i,f_j\oplus\beta_j}(a)\Big| &\leq [(2^n-1)\sum_{a\in\mathbb{F}_2^{n*}}(\sum_{i=1}^{m}\triangle_{f_i\oplus\beta_i,f_j\oplus\beta_j}(a))^2]^{1/2}\\
&= [(2^n-1)\sum_{a\in\mathbb{F}_2^{n}}[(\sum_{i=1}^{m}\triangle_{f_i\oplus\beta_i,f_j\oplus\beta_j}(a))^2\\
&\quad -(\sum_{i=1}^{m}\triangle_{f_i\oplus\beta_i,f_j\oplus\beta_j}(\mathbf{0}^n))^2]]^{1/2}\\
&= [(2^n-1)\sum_{a\in\mathbb{F}_2^{n}}(\sum_{i=1}^{m}\triangle_{f_i\oplus\beta_i,f_j\oplus\beta_j}(a))^2]^{1/2}.
\end{aligned}$$

Furthermore, we know

$$\sum_{a\in\mathbb{F}_2^{n}}(\sum_{i=1}^{m}\triangle_{f_i\oplus\beta_i,f_j\oplus\beta_j}(a))^2 \leq m\sum_{a\in\mathbb{F}_2^{n}}\sum_{i=1}^{m}[\triangle_{f_i\oplus\beta_i,f_j\oplus\beta_j}(a)]^2.$$

Thus,

$$\begin{aligned}
\sum_{a\in\mathbb{F}_2^{n*}}\sum_{j=1}^{m}\Big|\sum_{i=1}^{m}\triangle_{f_i\oplus\beta_i,f_j\oplus\beta_j}(a)\Big| &\leq \sum_{j=1}^{m}[m(2^n-1)\sum_{a\in\mathbb{F}_2^{n}}\sum_{i=1}^{m}[\triangle_{f_i\oplus\beta_i,f_j\oplus\beta_j}(a)]^2]^{1/2}\\
&= \sum_{j=1}^{m}[m(2^n-1)\sum_{i=1}^{m}\sum_{a\in\mathbb{F}_2^{n}}[\triangle_{f_i\oplus\beta_i,f_j\oplus\beta_j}(a)]^2]^{1/2}\\
&= \sum_{j=1}^{m}[m(2^n-1)\sum_{i=1}^{m}\sigma_{f_i\oplus\beta_i,f_j\oplus\beta_j}]^{1/2}\\
&\leq \sum_{j=1}^{m}[m(2^n-1)\sum_{i=1}^{m}\sqrt{\sigma_{f_i\oplus\beta_i}\sigma_{f_j\oplus\beta_j}}]^{1/2}\\
&= \sum_{j=1}^{m}[m(2^n-1)\sum_{i=1}^{m}\sqrt{\sigma_{f_i}\sigma_{f_j}}]^{1/2},
\end{aligned}$$

which gives a lower bound on $\mathcal{RTO}(F)$. ■

Theorem 4 gives the relationship between $\mathcal{RTO}(F)$ and $\sigma_{f_i}(1 \leq i \leq m)$, implying that the smaller the σ_{f_i} the larger is $\mathcal{RTO}(F)$. Using the fact that for any $f \in \mathbb{B}_n$, we have $\sigma_f \leq 2^n[\mathcal{L}_f]^2$ [15], where $\mathcal{L}_{f_i} = \max_{\alpha \in \mathbb{F}_2^n} \mid \mathcal{F}(f_i \oplus \varphi_\alpha) \mid$, one can easily deduce the following result.

Corollary 2. *Let $F = (f_1, \ldots, f_m)$ be a balanced (n, m)-function. If f_i and f_j are not almost perfectly uncorrelated for $1 \leq i \neq j \leq m$, then*

$$\mathcal{RTO}(F) \geq m - \sqrt{\frac{m}{2^n(2^n-1)}} \sum_{j=1}^{m} \left[\sum_{i=1}^{m} \mathcal{L}_{f_i} \mathcal{L}_{f_j} \right]^{1/2}.$$

Remark 3 *Using Theorem 4 and Corollary 2, one may also derive the relationship between $\mathcal{RTO}(F)$ and the nonlinearity of the coordinate functions N_{f_i}; alternatively between $\mathcal{RTO}(F)$ and the algebraic immunity $AI(f_i)$, where $1 \leq i \leq m$.*

1) The relationship between $\mathcal{RTO}(F)$ and $N_{f_i}(1 \leq i \leq m)$.

$$\mathcal{RTO}(F) \geq m - \sqrt{\frac{m}{2^n(2^n-1)}} \sum_{j=1}^{m} \left[\sum_{i=1}^{m} (2^n - 2N_{f_i})(2^n - 2N_{f_j}) \right]^{1/2}.$$

2) The relationship between $\mathcal{RTO}(F)$ and $AI(f_i)(1 \leq i \leq m)$.

$$\mathcal{RTO}(F) \geq m - \sqrt{\frac{m}{2^n(2^n-1)}} \sum_{j=1}^{m} \left\{ \sum_{i=1}^{m} \left[2^n - 4 \sum_{k=0}^{AI(f_i)-2} \binom{n-1}{k} \right] \left[2^n - 4 \sum_{l=0}^{AI(f_j)-2} \binom{n-1}{l} \right] \right\}^{1/2},$$

which easily follows from the bound $N_f \geq 2 \sum_{i=0}^{AI(f)-2} \binom{n-1}{i}$ for $f \in \mathbb{B}_n$, see [2, pp. 331].

In other words, the negative impact on $\mathcal{RTO}$ is again confirmed, thus the larger the N_{f_i} (or $AI(f_i)$), the larger is the $\mathcal{RTO}(F)$.

Finally, one can also deduce a lower bound on $\mathcal{RTO}$ which uses other cross-correlation properties of the coordinate functions.

Theorem 5. *Let $F = (f_1, \ldots, f_m)$ be a balanced (n, m)-function. If f_i and f_j are not almost perfectly uncorrelated for $1 \leq i \neq j \leq m$, then*

$$\mathcal{RTO}(F) \geq m - \frac{1}{2^n} \sum_{j=1}^{m} \sum_{i=1}^{m} (2^n - Num_{\triangle_{f_i,f_j}})(2^n - Num_{\mathcal{F}_{f_i,f_j}}),$$

where $Num_{\triangle_{f_i,f_j}} = \mid \{u \in \mathbb{F}_2^n : \triangle_{f_i,f_j}(u) = 0\} \mid$, $Num_{\mathcal{F}_{f_i,f_j}} = \left|\{u \in \mathbb{F}_2^n : \mathcal{F}(f_i \oplus \varphi_u)\mathcal{F}(f_j \oplus \varphi_u) = 0\}\right|$.

Proof. From [12], we know

$$\max_{a\in\mathbb{F}_2^n} \triangle_{f,g}(a) \leq (2^n - Num_{\triangle_{f,g}})(2^n - Num_{\mathcal{F}_{f,g}}).$$

Thus,

$$\begin{aligned}\sum_{a\in\mathbb{F}_2^{n*}} \mid \sum_{i=1}^{m} \triangle_{f_i\oplus\beta_i, f_j\oplus\beta_j}(a) \mid &\leq \sum_{a\in\mathbb{F}_2^{n*}} \sum_{i=1}^{m} \mid \triangle_{f_i\oplus\beta_i, f_j\oplus\beta_j}(a) \mid \\ &\leq (2^n-1)\sum_{i=1}^{m} \max_{a\in\mathbb{F}_2^n} \mid \triangle_{f_i\oplus\beta_i, f_j\oplus\beta_j}(a) \mid \\ &\leq (2^n-1)\sum_{i=1}^{m}(2^n - Num_{\triangle_{f_i,f_j}})(2^n - Num_{\mathcal{F}_{f_i,f_j}}) \\ &= (2^n-1)\sum_{i=1}^{m}(2^n - Num_{\triangle_{f_i,f_j}})(2^n - Num_{\mathcal{F}_{f_i,f_j}}).\blacksquare\end{aligned}$$

Remark 4 *In terms of the above results it is uncertain whether a design of cryptographic S-boxes satisfying all the relevant criteria (including the resistance to DPA attacks) is actually possible after all. The problem of giving a theoretical evidence regarding the existence of S-boxes with overall good properties remains open however. More specifically, the question is whether the induced trade-offs are acceptable from the security margins viewpoint or not.*

4 $\mathcal{RTO}$ of S-boxes of size 4×4

For efficient hardware implementation, small sized bijective S-boxes (as confusion primitives in block ciphers that use substitution permutation framework) are commonly preferable in practical applications. The number of bijective mappings $F : \mathbb{F}_2^4 \to \mathbb{F}_2^4$, up to affine equivalence (when a cryptographic property remains invariant under affine transformations; affine equivalent S-boxes share the same cryptographic properties), was determined. In [3], it was pointed out that $\mathcal{RTO}$ is affine invariant for $F \circ A$, where $A \in A_n$ is an affine permutation, and $\mathcal{RTO}$ is not affine invariant for $B \circ F$ under some affine permutation $B \in A_n$. The exact number of equivalence classes of 4×4 S-boxes is 302 among which only 10 S-boxes have nonlinearity 4, degree 3 and absolute auto-correlation value 8, which are the optimal values of these parameters for this particular size of the ambient space. For this reason the authors in [3] only provided the $\mathcal{RTO}$ values for these 10 equivalence classes of S-boxes. On the other hand, in [6], all optimal 4-bit S-boxes were classified and up to affine equivalence there are only 16 different classes (here "optimal" means that 16 classes S-boxes satisfy: 1) the linearity is 8 ; 2) the difference is 8; 3) the algebraic degree is 3), where the term optimal refers to those S-boxes that achieve the best differential property and nonlinearity.

4.1 $\mathcal{RTO}$ of 302 affine equivalent representative $(4, 4)$ S-box

We here compute the transparency order of all 302 (representative) S-boxes of size 4×4 and give a somewhat better insight in the behaviour of this parameter, especially with respect to randomly selected S-boxes. Our simulations show (see also [17]) that the transparency order is confined within the range $0 \leq \mathcal{RTO}(F) \leq 2.767$, having a single (affine) S-box, say F, for which $\mathcal{RTO}(F) = 0$. We summarize the distribution of transparency order values for $(4, 4)$ S-boxes in Table 3, omitting the case of affine S-boxes.

Table 3. Distribution of $\mathcal{RTO}$ for 302 $(4, 4)$ S-boxes [17]

$\mathcal{RTO}$	$Number$	$Per(\%)$	$\mathcal{RTO}$	$Number$	$Per(\%)$
0.467	1	0.331	2.133	6	1.656
0.800	1	0.331	2.167	2	0.662
1.067	1	0.331	2.200	2	0.662
1.133	1	0.331	2.233	1	0.331
1.267	1	0.331	2.267	6	1.656
1.333	3	0.993	2.300	5	1.656
1.400	1	0.331	2.333	22	7.285
1.533	1	0.331	2.367	15	4.967
1.600	1	0.331	2.400	22	7.285
1.733	2	0.662	2.433	21	6.954
1.800	4	1.325	2.467	30	9.934
1.833	1	0.331	2.500	31	10.265
1.867	5	1.656	2.533	30	9.934
1.900	1	0.331	2.567	26	8.609
1.933	8	2.649	2.600	20	6.623
1.967	3	0.993	2.633	9	2.980
2.000	2	0.662	2.667	7	2.318
2.033	1	0.331	2.700	1	0.331
2.067	3	0.993	2.733	1	0.331
2.100	2	0.662	2.767	1	0.331

Remark 5 *The number of affine equivalence classes whose transparency order lies in the range* $\mathcal{RTO}_{(4,4)} = [2.333, 2.600]$ *equals to* $217 = 22 + 15 + 22 + 21 + 30 + 31 + 30 + 26 + 20$*, which corresponds to about* 71.85% *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* $\mathcal{RTO}_{(4,4)}$ *is approximately* 71.85%*, which is quite high.*

4.2 $\mathcal{RTO}$ of $A \circ G_i$ for 16 optimal S-box G_i

From [6], we know that there are 16 different class (denoted by $G_0, G_1, \cdots, G_{15}$) in all optimal 4-bit S-boxes up to affine equivalence. Since $\mathcal{RTO}(S \circ A) =$

$\mathcal{RTO}(S)$ for any (n, n) S-box S and any affine permutation $A \in A_n$ [3], thus, we only analyse the distribution of $\mathcal{RTO}(A \circ G_i)(i = 0, 1, \cdots, 15)$. The number of affine permutation $A \in A_4$ is 20160, thus we calculate 20160 $\mathcal{RTO}(A \circ G_i)$ for every $G_i(i = 0, 1, \cdots, 15)$. Because the calculation method for the distribution of $\mathcal{RTO}(A \circ G_i)$ is similar for any $G_i(i = 0, 1, \cdots, 15)$, due to page limits, here we give the distribution of $\mathcal{RTO}(A \circ G_{15})$, where $G_{15} = \{0, 1, 2, 13, 4, 7, 15, 6, 8, 14, 12, 11, 9, 3, 10, 5\}$ [6], see Table 4.

Table 4. Distribution of $\mathcal{RTO}$ for $A \circ G_{15}$ S-boxes

Case	$\mathcal{RTO}$	$Number$	$Per(\%)$
1	2.133	24	0.119
2	2.167	72	0.357
3	2.200	144	0.714
4	2.233	312	1.55
5	2.267	144	0.714
6	2.300	432	2.143
7	2.333	600	2.976
8	2.367	1248	6.19
9	2.400	1848	9.167
10	2.433	2040	10.119
11	2.467	3000	14.881
12	2.500	2616	12.976
13	2.533	2904	14.404
14	2.567	1872	9.286
15	2.600	1296	6.429
16	2.633	672	3.333
17	2.667	360	1.786
18	2.700	288	1.429
19	2.733	144	0.714
20	2.767	48	0.238
21	2.800	24	0.119
22	2.867	48	0.238
23	2.900	24	0.119
–	–	20160	100

Remark 6 *From Table 4, we can find that there are 23 different value for* $\mathcal{RTO}(A \circ G_{15})$*. The range of* $\mathcal{RTO}(A \circ G_{15})$ *is* $[2.133, 2.900]$*, but* $\mathcal{RTO}(G_{15}) = 2.500$*. This shows that some affine permutation* A *makes* $\mathcal{RTO}(A \circ G_i) > \mathcal{RTO}(G_i)$*, certain* A *make* $\mathcal{RTO}(A \circ G_i) < \mathcal{RTO}(G_i)$*, and it can happen that* $\mathcal{RTO}(A \circ G_i) = \mathcal{RTO}(G_i)$ *for* $i = 0, 1, \cdots, 15$*. This further implies that* $\mathcal{RTO}$ *is not an invariant with respect to an affine permutation. This fact is consistent with the results in [6].*

5 Conclusions

This article further addresses some relevant results related to $\mathcal{TO}$ and $\mathcal{RTO}$. We answer the open problem regarding the existence of (n, m)-functions that reach the upper bound on $\mathcal{TO}$ for odd n, and give tight upper and lower bounds $\mathcal{RTO}$. Then, we derive its relationship to main cryptographic characterizations of (n, m)-functions (such as nonlinearity, the sum-of-square indicator and algebraic immunity). Finally, the distributions of $\mathcal{RTO}$ for 302 4-bit S-boxes and $\mathcal{RTO}$ of $A \circ G_i$ for 16 optimal S-box G_i are given as theoretical verification. These results improve the theoretical results for $\mathcal{RTO}$ of S-boxes, and lay a theoretical foundation for how to construct S-boxes with smaller $\mathcal{RTO}$ in the next step.

Acknowledgments

Yu Zhou is supported in part by the Sichuan Science and Technology Program (2020JDJQ0076). Yongzhuang Wei is supported by the National Natural Science Foundation of China (61872103), the Guangxi Science and Technology Foundation (Guike AB18281019) and the Guangxi Natural Science Foundation (2019GXNSFGA245004). Hailong Zhang is supported by the National Natural Science Foundation of China (61872040). Enes Pasalic is supported in part by the Slovenian Research Agency (research program P1-0404 and research projects J1-9108, J1-1694, N1-0159, J1-2451). Luyang Li is supported by the Natural Science Foundation of Shaanxi Provincial Department of Education (20JK0911).

References

1. C. Carlet.: On Highly Nonlinear S-Boxes and Their Inability to Thwart DPA Attacks. INDOCRYPT 2005, LNCS 3797, pp. 49-62 (2005)
2. C. Carlet.: Boolean Functions for Cryptography and Coding Theory, Cambridge University Press (2020)
3. K. Chakraborty, S. Sarkar, S. Maitra, B. Mazumdar, D. Mukhopadhyay, and E. Prouff.: Redefining the Transparency Order. Designs Codes and Cryptography **82**(1-2) : 95–115 (2017)
4. L. Fan, Y. Zhou, D. Feng.: A fast implementation of computing the transparency order of S-Boxes. The 9th International Conference of Young Computer Scientists, 2008, ICYCS 2008. IEEE, 2008, pp. 206–211 (2008)
5. P. Kocher, J. Jaffe, and B. Jun.: Differential Power Analysis. In Michael Wiener, editor, Advances in Cryptology — CRYPTO' 99, Springer Berlin Heidelberg, pp. 388–397 (1999)
6. G. Leander, A. Poschmann.: On the Classification of 4 bit S-Boxes. WAIFI, pp. 159–176 (2007)
7. B. Mazumdar, D. Nyjgioadgtat, I. Sengupta.: Constrained search for a class of good bijective S-boxes with improved DPA resistivity. IEEE Transactions on Information Forensics and Security **8**(12): 2154–2163 (2013)

8. E. Pasalic, S. Maitra, T. Johansson, and P. Sarkar.: New Constructions of Resilient and Correlation Immune Boolean Functions Achieving Upper Bound on Nonlinearity. Electronic Notes in Discrete Mathematics **6**: 158–167 (2001)
9. S. Picek, L. Batina, D.Jakobovic.: Evolving DPA-Resistant Boolean functions. International Conference on Parallel Problem Solving from Nature' 2014, Springer-Verlag. LNCS **8672**: 812–821 (2014)
10. E. Prouff.: DPA Attacks and S-Boxes. In Fast Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers, pp. 424–441 (2005)
11. O. S. Rothaus.: On bent functions. Journal of Combinatorial Theory A (**20**): 300–305 (1976)
12. P. Sarkar and S. Maitra.: Cross-Correlation Analysis of Cryptographically Useful Boolean Functions and S-Boxes. Theory of Computing Systems **35**(1): 39–57 (2002)
13. Q. Wang and P. Stănică.: Transparency order for Boolean functions: analysis and construction. Designs Codes and Cryptography **87**: 2043–2059 (2019)
14. X. Zhang and Y. Zheng.: GAC - the Criterion for Global Avalance Characteristics of Cryptographic Functions. Journal of Universal Computer Science **1**(5): 320–337 (1995)
15. Y. Zheng and X. Zhang.: On Plateaued Functions. IEEE Transactions on Information Theory **47**(3): 1215-1223 (2001)
16. Y. Zhou, M. Xie, and G. Xiao.: On the global avalanche characteristics between two Boolean functions and the higher order nonlinearity. Information Sciences **180**(2): 256–265 (2010)
17. Y. Zhou, Y. Wei, H. Zhang, W. Zhang.: On the modified transparency order of (n, m)-functions. Security and Communication Networks. https://doi.org/10.1155/2021/6640099 (in press)