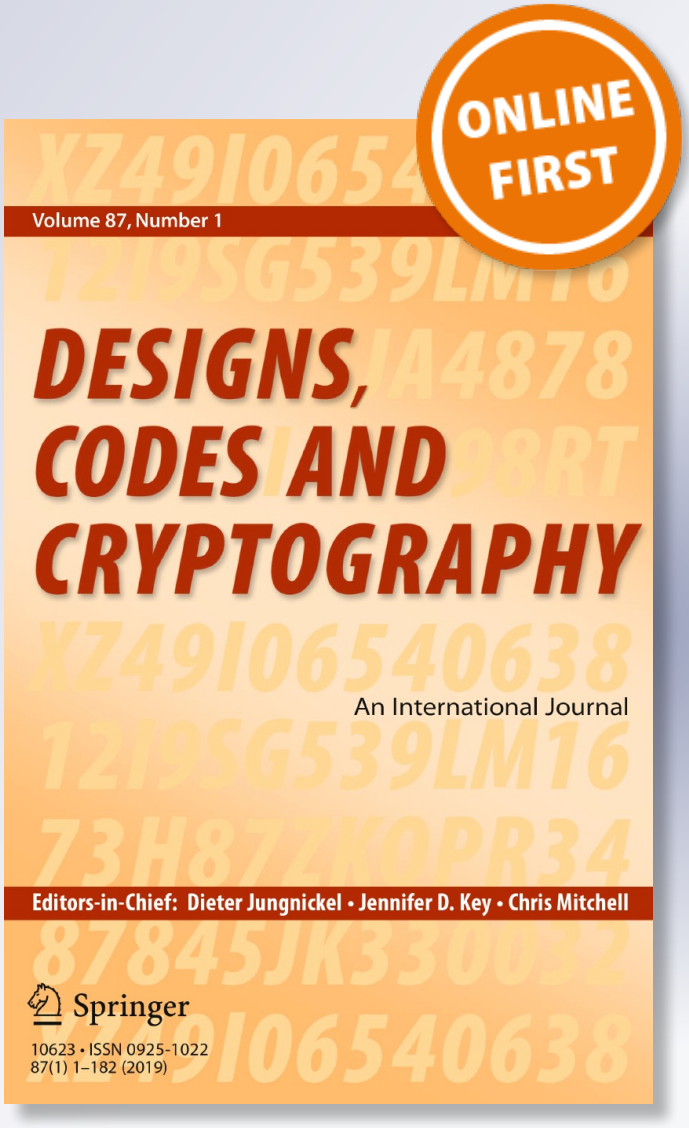
Transparency order for Boolean functions: analysis and construction

Qichun Wang & Pantelimon Stănică

Designs, Codes and Cryptography
An International Journal

ISSN 0925-1022

Des. Codes Cryptogr.
DOI 10.1007/s10623-019-00604-1



Springer

Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-019-00604-1

Transparency order for Boolean functions: analysis and construction

Qichun Wang[1] · **Pantelimon Stănică**[2]

Received: 4 April 2018 / Revised: 3 October 2018 / Accepted: 2 January 2019

Abstract
The notion of transparency order, proposed by Prouff (DPA attacks and S-boxes, FSE 2005, LNCS 3557, Springer, Berlin, 2005) and then redefined by Chakraborty et al. (Des Codes Cryptogr 82:95–115, 2017), is a property that attempts to characterize the resilience of cryptographic algorithms against differential power analysis attacks. In this paper, we give a tight upper bound on the transparency order in terms of nonlinearity, inferring the worst possible transparency order of those functions with the same nonlinearity. We also give a lower bound between transparency order and nonlinearity. We study certain classes of Boolean functions for their transparency order and find that this parameter for some functions of low algebraic degree can be determined by their nonlinearity. Finally, we construct two infinite classes of balanced semibent Boolean functions with provably relatively good transparency order (this is the first time that an infinite class of highly nonlinear balanced functions with provably good transparency order is given).

Keywords Transparency order · Boolean function · Nonlinearity

Mathematics Subject Classification 11T71 · 11L03

1 Introduction

Side-channel analysis (SCA) is a very powerful technique which targets implementations of block ciphers [17]. Differential power analysis (DPA) [18] is a form of SCA, which studies the power consumption of a cryptographic hardware device (it involves statistical

Communicated by C. Carlet.

✉ Qichun Wang
qcwang@fudan.edu.cn

Pantelimon Stănică
pstanica@nps.edu

[1] School of Computer Science and Technology, Nanjing Normal University, Nanjing 210046, People's Republic of China

[2] Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943-5216, USA

Published online: 09 January 2019

analysis and error correction techniques to extract information correlated to secret keys, which involves data collection by capturing power traces corresponding to some ciphertexts and data analysis computing differential traces). DPA relies on the leakages from physical hardware implementations, and is more efficient than the differential or linear cryptanalysis [3,21]. To improve the resistance of a block cipher to DPA, some countermeasures have been proposed, such as hiding and masking schemes [21]. However, those countermeasures are extremely costly due to area overhead and throughput loss, and is therefore impractical for resource constrained devices [26].

As the only nonlinear part in many ciphers, the S-box is fundamental for the security of the cipher, and its cryptographic properties should be good. For assessing the behavior of an S-box against SCA, several properties were proposed. First property related with SCA was introduced in 2004, called SNR (Signal-to-Noise Ratio) DPA [14]. In 2005, Prouff [32] proposed the notion of transparency order which characterizes the resistance of an S-box to DPA attacks. Later, Fei [10,11] introduced the notion of confusion coefficient. Very recently, Chakraborty et al. [7] found that the original definition had flaws and redefined the transparency order (a low transparency order is desired). They confirmed practically that the revised transparency order has impact on the resistance of the implementation against DPA attacks. The challenge is that highly nonlinear S-boxes have higher transparency order (not desired), implying that they are more susceptible to DPA attacks, while linear S-boxes are good in terms of transparency order but cannot be used for other cryptographic reasons. It should be noted that the revised transparency order is still inadequate to gauge the side channel robustness, but gives an indication. However, though it does not rule out DPA, a proper choice of the transparency order can lead to less overheads in the countermeasures, such as masking, as shown in Sect. 6 of [26].

DPA is also a real threat for stream ciphers. In 2006, Fischer et al. [13] made use of the nonlinear part of Grain and presented a DPA attack on this cipher. The nonlinear combiner and the filter generator are two well studied models of stream cipher [6]. In these two models, the Boolean function is the only nonlinear part and should have good cryptographic properties: balancedness, high algebraic degree, high algebraic immunity, high nonlinearity, correlation immunity and good immunity to fast algebraic attacks. Moreover, it should have good resistance to DPA attacks. If the other cryptographic properties of two functions are equivalent, then a designer can choose the function with a better transparency order.

1.1 Related work

As already pointed out, a low transparency order of an S-box is considered to be good. In the same year when this notion was proposed, Carlet [3] showed that some highly nonlinear S-boxes constructed using power maps have very bad transparency orders. However, it seems that this new notion did not receive enough attention until 2013. Since then, many papers revisited this topic (see e.g. [9,22–25,28–31,34,35]), and constructed some 4×4 and 8×8 S-boxes with relatively good transparency orders using search algorithms.

The transparency order of Boolean functions was firstly considered by Picek et al. [27], and some 8-variable Boolean functions with good nonlinearity and relatively good transparency order were found using evolutionary algorithms. In 2015, using similar evolutionary algorithms, Jain and Chaudhari [16] found three 8-variable highly nonlinear balanced Boolean functions that have lower transparency orders than the ones of [27].

So far, little attempt has been made to analyze theoretically the transparency order, and all constructions related to the transparency order are based on search algorithms and with only up to 8 variables.

1.2 Our contribution

In this paper, we give a tight upper bound on transparency order in terms of nonlinearity, inferring the worst possible transparency order of those functions with the same nonlinearity. We also give a lower bound between transparency order and nonlinearity. We study certain classes of Boolean functions for their transparency order and find that this parameter for some functions of low algebraic degree can be determined by their nonlinearity. From the above results, for most cases, the transparency order will increase as the value of nonlinearity increases. In other words, the transparency order and nonlinearity cannot be both good in the same time. However, given some nonlinearity, we can choose a function with relative good transparency order, given the unavoidable trade-off. Finally, we construct two infinite classes of balanced semibent Boolean functions with provably relatively good transparency order (this is the first time that an infinite class of highly nonlinear balanced functions with provably good transparency order is given).

The paper is organized as follows. In Sect. 2, the necessary background is established. In Sect. 3, we deduce the upper and lower bounds on the transparency order in terms of the nonlinearity. In Sect. 4, we prove that the transparency order of some functions with low degree can be determined by their nonlinearity and then give some experimental results on the transparency order of some cryptographic Boolean functions in Sect. 5. In Sect. 6, we investigate how the transparency order behaves on concatenations. In Sect. 7, we construct two infinite classes of balanced semibent Boolean functions with provably relatively good transparency order. We end in Sect. 8 with conclusions.

2 Preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the finite field $\mathbb{F}_2$. We denote by $\mathcal{B}_n$ the set of all n-variable Boolean functions, from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. Any Boolean function $f \in \mathcal{B}_n$ can be uniquely represented as a multivariate polynomial in $\mathbb{F}_2[x_1, \ldots, x_n]$,

$$f(x_1, \ldots, x_n) = \sum_{K \subseteq \{1,2,\ldots,n\}} a_K \prod_{k \in K} x_k,$$

which is called the *algebraic normal form* (ANF) of f. The *algebraic degree* of f, denoted by $\deg(f)$, is the number of variables in the highest order term with nonzero coefficient. A Boolean function is *affine* if there exists no term of degree strictly greater than 1 in the ANF. The set of all affine functions is denoted by A_n.

Let $1_f = \{x \in \mathbb{F}_2^n | f(x) = 1\}$ be the support of a Boolean function f, whose cardinality $|1_f|$ is called the *Hamming weight* of f, and will be denoted by $wt(f)$. The *Hamming distance* between two functions f and g, denoted by $d(f, g)$, is the Hamming weight of $f + g$. We say that an n-variable Boolean function f is *balanced* if $wt(f) = 2^{n-1}$. Let $f \in \mathcal{B}_n$. The *nonlinearity* [4,8] of f is

$$nl(f) = \min_{g \in A_n} d(f, g).$$

The nonlinearity of an n-variable Boolean function is bounded above by $2^{n-1} - 2^{n/2-1}$, and a function is said to be *bent* if it achieves this bound.

The *Walsh–Hadamard transform* of a given function $f \in \mathcal{B}_n$ is the integer-valued function over $\mathbb{F}_2^n$ defined by

$$\mathcal{W}_f(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\omega \cdot x},$$

where $\omega \in \mathbb{F}_2^n$ and $\omega \cdot x$ is an inner product, for instance, $\omega \cdot x = \omega_1 x_1 + \omega_2 x_2 + \cdots + \omega_n x_n$. It is easy to see that a Boolean function f is balanced if and only if $\mathcal{W}_f(0) = 0$. Moreover, the nonlinearity of f can be determined by

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_2^n} |\mathcal{W}_f(\omega)|.$$

Let $F = (F_1, \ldots, F_m)$, $F_i \in \mathcal{B}_n$, be a vectorial function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. The *transparency order* [7] of F is defined by

$$TO(F) = \max_{\beta \in \mathbb{F}_2^m} \left(m - \frac{1}{2^{2n} - 2^n} \sum_{y \in \mathbb{F}_2^{n*}} \sum_{j=1}^{m} \left| \sum_{i=1}^{m} (-1)^{\beta_i \oplus \beta_j} \mathcal{C}_{F_i, F_j}(y) \right| \right),$$

where

$$\mathcal{C}_{F_i, F_j}(y) = \sum_{x \in \mathbb{F}_2^n} (-1)^{F_i(x) \oplus F_j(x \oplus y)},$$

is the *correlation* between F_i, F_j (if $F_i = F_j$, we shall use the notation $\mathcal{C}_{F_i}$ and call it the *autocorrelation* of F_i). If $m = 1$, then F is a Boolean function, and

$$TO(F) = 1 - \frac{1}{2^n (2^n - 1)} \sum_{y \in \mathbb{F}_2^{n*}} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{F(x) \oplus F(x \oplus y)} \right|.$$

Clearly, $TO(F)$ is affine invariant [7]. It is noted that the revised transparency order and the original transparency order are the same for Boolean functions [32].

Further, recall that $f \in \mathcal{B}_n$ is called *plateaued* if $|\mathcal{W}_f(u)| \in \{0, 2^{(n+s)/2}\}$ for all $u \in \mathbb{F}_2^n$ for a fixed integer s depending on f (we also then call f *s-plateaued*). If $s = 1$ (n must then be odd), or $s = 2$ (n must then be even), we call f *semibent*.

We use $||$ to denote the concatenation, i.e., $(f_1||f_2)(x_1, \ldots, x_n, x_{n+1}) = f_1(x_1, \ldots, x_n) \oplus x_{n+1}(f_1(x_1, \ldots, x_n) \oplus f_2(x_1, \ldots, x_n))$.

The following two lemmas will be used afterwards, and are direct consequences of Poisson summation formula (see e.g. [4]).

Lemma 2.1 *Let $f \in \mathcal{B}_n$. Then for any $y \in \mathbb{F}_2^n$,*

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus y)} = \frac{1}{2^n} \sum_{u \in \mathbb{F}_2^n} (-1)^{u \cdot y} \mathcal{W}_f^2(u).$$

Lemma 2.2 *Let $f \in \mathcal{B}_n$. Then for any $v \in \mathbb{F}_2^n$,*

$$\sum_{y \in \mathbb{F}_2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus y) \oplus v \cdot y} = \mathcal{W}_f^2(v).$$

3 Transparency order and nonlinearity

3.1 An upper bound of the transparency order

It was observed in [7] that linear functions have the lowest transparency order and high nonlinear functions tend to have worse transparency order. The question that arises is to find some connection between transparency order and nonlinearity. In our next result, we give an upper bound for the transparency order in terms of nonlinearity, inferring the worst possible transparency order of those functions with the same nonlinearity.

Theorem 3.1 *Let $f \in \mathcal{B}_n$. Then*

$$TO(f) \leq 1 - \frac{(2^n - 2nl(f))^2}{2^n(2^n-1)} + \frac{1}{2^n-1}.$$

Proof Clearly, for any $v \in \mathbb{F}_2^n$, we have

$$\begin{aligned}\sum_{y\in\mathbb{F}_2^{n*}} \left|\sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus f(x\oplus y)}\right| &= \sum_{y\in\mathbb{F}_2^{n*}} \left|(-1)^{v\cdot y}\sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus f(x\oplus y)}\right| \\ &\geq \left|\sum_{y\in\mathbb{F}_2^n}\sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus f(x\oplus y)\oplus v\cdot y} - 2^n\right|.\end{aligned}$$

Then by Lemma 2.2,

$$\sum_{y\in\mathbb{F}_2^{n*}} \left|\sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus f(x\oplus y)}\right| \geq |\mathcal{W}_f^2(v) - 2^n|.$$

Therefore,

$$\sum_{y\in\mathbb{F}_2^{n*}} \left|\sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus f(x\oplus y)}\right| \geq \max_{v\in\mathbb{F}_2^n} \mathcal{W}_f^2(v) - 2^n = (2^n - 2nl(f))^2 - 2^n,$$

and the result follows. □

We now show that the upper bound of Theorem 3.1 is tight. We define the Walsh–Hadamard spectrum support $\Lambda_f := \{u \in \mathbb{F}_2^n \mid \mathcal{W}_f(u) \neq 0\}$ and use the notation $L_f(y) := \sum_{u\in\Lambda_f} (-1)^{u\cdot y}$.

Theorem 3.2 *Let $f \in \mathcal{B}_n$. If $nl(f) \leq 2^{n-1} - 2^{n-\frac{3}{2}}$ or $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$, then*

$$TO(f) = 1 - \frac{(2^n - 2nl(f))^2}{2^n(2^n-1)} + \frac{1}{2^n-1}.$$

If f is s-plateaued, then

$$TO(f) = 1 - \frac{1}{2^{n-s}(2^n-1)} \sum_{y\in\mathbb{F}_2^{n*}} |L_f(y)|.$$

Proof If $nl(f) \le 2^{n-1} - 2^{n-\frac{3}{2}}$, then we have

$$\max_{\omega \in \mathbb{F}_2^n} |\mathcal{W}_f(\omega)| \ge 2^{n-\frac{1}{2}}.$$

Let $v \in \mathbb{F}_2^n$ and $|\mathcal{W}_f(v)| = \max_{\omega \in \mathbb{F}_2^n} |\mathcal{W}_f(\omega)|$. Since $\sum_{u \in \mathbb{F}_2^n} \mathcal{W}_f^2(u) = 2^{2n}$, we have

$$\mathcal{W}_f^2(v) \ge 2^{2n-1} \ge \sum_{u \ne v} \mathcal{W}_f^2(u).$$

Then by Lemma 2.1, for any $y \in \mathbb{F}_2^n$, we have

$$\begin{aligned} 2^n (-1)^{v \cdot y} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus y)} &= \sum_{u \in \mathbb{F}_2^n} (-1)^{(u \oplus v) \cdot y} \mathcal{W}_f^2(u) \\ &= \mathcal{W}_f^2(v) + \sum_{u \ne v} (-1)^{(u \oplus v) \cdot y} \mathcal{W}_f^2(u) \ge 0. \end{aligned}$$

If $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$, then f is a bent function. In this case, for any $y \in \mathbb{F}_2^{n*}$, we have

$$(-1)^{v \cdot y} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus y)} = 0.$$

Therefore, if $nl(f) \le 2^{n-1} - 2^{n-\frac{3}{2}}$ or $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$, then by Lemma 2.2,

$$\begin{aligned} \sum_{y \in \mathbb{F}_2^{n*}} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus y)} \right| &= \sum_{y \in \mathbb{F}_2^{n*}} \left| (-1)^{v \cdot y} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus y)} \right| \\ &= \sum_{y \in \mathbb{F}_2^{n*}} (-1)^{v \cdot y} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus y)} \\ &= \mathcal{W}_f^2(v) - 2^n = \left(2^n - 2nl(f)\right)^2 - 2^n, \end{aligned}$$

and the first claim follows.

Next, if f is s-plateaued, using Lemma 2.1 and the fact that the cardinality $\#\left\{u \,|\, \mathcal{W}_f(u) = \pm 2^{\frac{n+s}{2}}\right\} = \#\Lambda_f = 2^{n-s}$, we get

$$\begin{aligned} TO(f) &= 1 - \frac{1}{2^n(2^n-1)} \sum_{y \in \mathbb{F}_2^{n*}} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus y)} \right| \\ &= 1 - \frac{1}{2^{2n}(2^n-1)} \sum_{y \in \mathbb{F}_2^{n*}} \left| \sum_{u \in \mathbb{F}_2^n} (-1)^{u \cdot y} \mathcal{W}_f^2(u) \right| \\ &= 1 - \frac{2^{n+s}}{2^{2n}(2^n-1)} \sum_{y \in \mathbb{F}_2^{n*}} \left| \sum_{u \in \Lambda_f} (-1)^{u \cdot y} \right| \\ &= 1 - \frac{1}{2^{n-s}(2^n-1)} \sum_{y \in \mathbb{F}_2^{n*}} |L_f(y)|, \end{aligned}$$

and the proof of the theorem is done. □

3.2 A lower bound of the transparency order

We now give a lower bound for the transparency order.

Theorem 3.3 *Let $f \in \mathcal{B}_n$ and $nl(f) \geq 2^{n-1} - C \cdot 2^{\frac{n}{2}} \geq 0$, where $C > 0$ is a constant. Then*

$$TO(f) \geq 1 - \frac{\sqrt{16C^4 - 1}}{\sqrt{2^n - 1}}.$$

Clearly, $TO(f) \to 1$, if $n \to \infty$.

Proof By Lemma 2.1, we have

$$\begin{aligned}\sum_{y\in\mathbb{F}_2^n}\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)\oplus f(x\oplus y)}\right)^2 &= \sum_{y\in\mathbb{F}_2^n}\left(\frac{1}{2^n}\sum_{u\in\mathbb{F}_2^n}(-1)^{u\cdot y}\mathcal{W}_f^2(u)\right)^2\\ &= \frac{1}{2^{2n}}\sum_{u,v\in\mathbb{F}_2^n}\mathcal{W}_f^2(u)\mathcal{W}_f^2(v)\sum_{y\in\mathbb{F}_2^n}(-1)^{(u\oplus v)\cdot y}\\ &= \frac{1}{2^n}\sum_{u\in\mathbb{F}_2^n}\mathcal{W}_f^4(u) \leq \max_{u\in\mathbb{F}_2^n}\mathcal{W}_f^4(u).\end{aligned}$$

Therefore,

$$\sum_{y\in\mathbb{F}_2^{n*}}\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)\oplus f(x\oplus y)}\right)^2 \leq (2^n - 2nl(f))^4 - 2^{2n} \leq (16C^4 - 1)2^{2n}.$$

Hence,

$$\begin{aligned}\left(\sum_{y\in\mathbb{F}_2^{n*}}\left|\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)\oplus f(x\oplus y)}\right|\right)^2 &\leq (2^n - 1)\sum_{y\in\mathbb{F}_2^{n*}}\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)\oplus f(x\oplus y)}\right)^2\\ &\leq (2^n - 1)(16C^4 - 1)2^{2n},\end{aligned}$$

and the result follows. □

Corollary 3.4 *If f is an s-plateaued function, then*

$$1 - \sqrt{\frac{2^{2s} - 1}{2^n - 1}} \leq TO(f) \leq 1 - \frac{2^s - 1}{2^n - 1}.$$

Proof By taking $C = 2^{\frac{s}{2}-1}$ in the theorem above, we obtain the lower bound. Since $nl(f) = 2^{n-1} - 2^{\frac{n+s}{2}-1}$, the upper bound follows from Theorem 3.1. □

We note that if n is large and the nonlinearity of f is high, then the lower bound of Theorem 3.3 shows that $TO(f)$ is not good. In other words, transparency order and nonlinearity of a Boolean function cannot be both good.

Table 1 Comparison among 5-variable functions

$nl(f)$	Exact value of $TO(f)$	Upper bound	Lower bound
0	0	0	0
1	0.1250	0.1250	0
2	0.2419	0.2419	0
3	0.3508	0.3508	0
4	0.4516	0.4516	0
5	0.5444	0.5444	0
6	0.6290	0.6290	0
7	0.7056	0.7056	0
8	0.7742	0.7742	0
9	$0.7540 \le T_f \le 0.8105$	0.8347	0
10	$0.7258 \le T_f \le 0.8871$	0.8871	0.2120
11	$0.8266 \le T_f \le 0.8508$	0.9315	0.4682
12	0.9677 or 0.9355	0.9677	0.6889

3.3 Some numerical experiments

For $n = 5$, the classification of Boolean functions under the affine group has been fully studied (see [19,20]). We computed $nl(f_i)$ and $TO(f_i)$ for representatives of all those affine equivalence classes and summarize the results in Table 1. From this table we see that if $nl(f_i) \le 8$, then $TO(f_i)$ equals our upper bound. Moreover, for $0 \le m \le 6$, there exists f_i of nonlinearity $2m$ such that $TO(f_i)$ achieves our upper bound.

In Table 1, we also give the lower bound of $TO(f)$, for $n = 5$. From the table, if $nl(f) = 12$, then we have $TO(f) \ge 0.689$. But the exact value of $TO(f)$ is either 0.968 or 0.936. There seems to be a big gap between the lower bound and the exact value of $TO(f)$.

For $n = 6$, there are 15,768,919 affine equivalence classes [15], and it is impractical to compute $nl(f_i)$ and $TO(f_i)$ for representatives of all these affine equivalence classes. We made some numerical experiments and it seems that the following conjecture holds.

Conjecture 3.5 *Let $f \in \mathcal{B}_n$ and $wt(f)$ be an even number. Then*

$$\max_{\substack{g\in\mathcal{B}_n \\ nl(g)=nl(f)}} TO(g) = 1 - \frac{(2^n - 2nl(f))^2}{2^n(2^n-1)} + \frac{1}{2^n-1}.$$

4 Transparency order of some Boolean functions with low degree

We now show that the transparency order of some low algebraic degree functions attains the bound given by Theorem 3.1.

Theorem 4.1 *The following functions all achieve the upper bound of Theorem 3.1:*

(i) *If $f \in \mathcal{B}_n$ be a quadratic function, then*

$$TO(f) = 1 - \frac{(2^n - 2nl(f))^2}{2^n(2^n-1)} + \frac{1}{2^n-1}.$$

(ii) *If $f \in \mathcal{B}_n$ is any cubic symmetric $f = s_3 + \lambda_2 s_2 + \lambda_1 s_1$, where s_i are the elementary symmetric polynomials of degree i, and $\lambda_i \in \mathbb{F}_2$, $1 \le i \le 3$, then*

$$TO(f) = 1 - \frac{(2^n - 2nl(f))^2}{2^n(2^n-1)} + \frac{1}{2^n - 1}.$$

(iii) *If $f \in \mathcal{B}_n$ is the elementary symmetric polynomials of degree 4, where $n \equiv 1 \pmod 4$, then*

$$TO(f) = 1 - \frac{(2^n - 2nl(f))^2}{2^n(2^n-1)} + \frac{1}{2^n - 1}.$$

Proof When f is quadratic, it is well known that f is affine equivalent to a function of the form $f_1 = x_1x_2 \oplus \cdots \oplus x_{2p-1}x_{2p}$ or $f_2 = x_1x_2 \oplus \cdots \oplus x_{2q-1}x_{2q} \oplus x_{2q+1}$, where $p \le \frac{n}{2}$ and $q \le \frac{n-1}{2}$. Clearly, $nl(f_1) = (2^{2p-1} - 2^{p-1})2^{n-2p}$ and $nl(f_2) = (2^{2q-1} - 2^{q-1})2^{n-2q}$. Let $y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_2^n$. We have

$$\left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f_1(x) \oplus f_1(x \oplus y)} \right| = \begin{cases} 2^n, & \text{if } \prod_{1 \le i \le 2p} (y_i \oplus 1) = 1, \\ 0, & \text{otherwise,} \end{cases}$$

and

$$\left| \sum_{x \in \mathbb{F}_2^n} (-1)^{f_2(x) \oplus f_2(x \oplus y)} \right| = \begin{cases} 2^n, & \text{if } \prod_{1 \le i \le 2q} (y_i \oplus 1) = 1, \\ 0, & \text{otherwise,} \end{cases}$$

Therefore,

$$TO(f_2) = 1 - \frac{1}{2^n(2^n-1)} 2^n (2^{n-2q} - 1) = 1 - \frac{2^{n-2q} - 1}{2^n - 1}.$$

If $n > 2p$, then

$$TO(f_1) = 1 - \frac{1}{2^n(2^n-1)} 2^n (2^{n-2p} - 1) = 1 - \frac{2^{n-2p} - 1}{2^n - 1},$$

and the first claim follows.

Next, if f is any cubic symmetric, then from TABLE III of [2], $\mathcal{C}_f(y) \ge 0$, when $wt(y)$ is even. Moreover, $\mathcal{C}_f(y)$ is a constant, if $wt(y)$ is odd. Therefore, there is a $v = (0, \ldots, 0)$ or $(1, \ldots, 1)$ such that

$$\sum_{y \in \mathbb{F}_2^{n*}} |\mathcal{C}_f(y)| = \sum_{y \in \mathbb{F}_2^{n*}} (-1)^{v \cdot y} \mathcal{C}_f(y).$$

Then by Lemma 2.2,

$$TO(f) = 1 - \frac{\mathcal{W}_f^2(v) - 2^n}{2^n(2^n-1)} \ge 1 - \frac{(2^n - 2nl(f))^2}{2^n(2^n-1)} + \frac{1}{2^n - 1}.$$

Hence, by Theorem 3.1, the second claim follows.

We now show the last claim. It is easy to check that

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus y)} > 0,$$

Table 2 Transparency order of the majority function

n	nl	The upper bound	$TO(MF)$
5	10	0.8871	0.7258
6	22	0.9167	0.8333
7	44	0.9094	0.8268
8	93	0.9289	0.8042
9	186	0.9270	0.8027
10	386	0.9404	0.8538
11	772	0.9399	0.8534
12	1586	0.9493	0.8422

for any $y \in \mathbb{F}_2^n$. Therefore, by Lemma 2.2,

$$\sum_{y\in\mathbb{F}_2^{n*}} |\mathcal{C}_f(y)| = \sum_{y\in\mathbb{F}_2^n} (-1)^{0\cdot y}\mathcal{C}_f(y) - 2^n = \mathcal{W}_f^2(0) - 2^n.$$

Hence,

$$\begin{aligned} TO(f) &= 1 - \frac{\mathcal{W}_f^2(0) - 2^n}{2^n(2^n-1)} \\ &\geq 1 - \frac{(2^n - 2nl(f))^2}{2^n(2^n-1)} + \frac{1}{2^n-1}, \end{aligned}$$

and the last claim follows. □

It should be noted that there are many cubic functions whose transparency orders are lower than the upper bound. For example, $x_1x_2x_5 \oplus x_1x_3x_4 \oplus x_2x_3$ is a 5-variable function with the nonlinearity 10. Its transparency order is 0.823, while the upper bound is 0.887.

If $n \equiv 1 \pmod 4$, then the transparency order of the n-variable elementary symmetric polynomials of degree 4 is the same as the upper bound. For other cases, its transparency order may be good. For example, if $n = 6$ or 7, then the elementary symmetric polynomials of degree 4 is the majority function, and its transparency order is much lower than the upper bound given by Theorem 3.1.

5 Experimental results on the transparency order of some cryptographic Boolean functions

We now present some experimental results related to the transparency order of some Boolean functions.

The majority function Let $MF \in \mathcal{B}_n$ be the majority function. That is, $MF(x) = 1$ if and only if $wt(x) > \frac{n}{2}$. We computed the transparency order of the majority function, for $5 \leq n \leq 12$ and compare it with the upper bound given by Theorem 3.1 (see Table 2). For $n = 5$, the majority function has the lowest transparency order among all those functions with the nonlinearity 10. For $n > 5$, we do not know whether it still can achieve the lowest transparency order. But it seems that the transparency order of MF is also quite good compared to functions with the same nonlinearity.

Table 3 Transparency order of the hidden weighted bit function

n	nl	The upper bound	$TO(HWBF)$
5	10	0.8871	0.8387
6	20	0.8730	0.8492
7	44	0.9094	0.8720
8	88	0.9059	0.8814
9	186	0.9270	0.8977
10	372	0.9261	0.9052
11	772	0.9399	0.9156
12	1544	0.9397	0.9202

Table 4 Transparency order of the Carlet–Feng function

n	nl	The upper bound	$TO(CF)$
5	10	0.8871	0.8710
6	24	0.9524	0.9048
7	54	0.9833	0.9380
8	112	0.9882	0.9564
9	232	0.9932	0.9691
10	484	0.9980	0.9823
11	984	0.9990	0.9866
12	1994	0.9995	0.9922

The hidden weighted bit function Let $HWBF \in \mathcal{B}_n$ be the hidden weighted bit function. That is [1,42],

$$HWBF(x) = \begin{cases} 0 & \text{if } x = 0 \\ x_{wt(x)} & \text{otherwise.} \end{cases}$$

It is known that $HWBF$ can be implemented very efficiently and has acceptable cryptographic properties. We computed the transparency order of $HWBF$, for $5 \leq n \leq 12$ and compare it with the upper bound given by Theorem 3.1 (see Table 3). Comparing with the majority function, $TO(HWBF)$ is weaker, since $nl(HWBF) \leq nl(MF)$ and $TO(HWBF)$ is much higher than $TO(MF)$.

The Carlet–Feng function The Carlet–Feng function $CF \in \mathcal{B}_n$ is defined as the function with support [5,12]

$$1_{CF} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^{n-1}-2}\},$$

where $\alpha \in \mathbb{F}_{2^n}$ is a primitive element. It is known that CF has quite good cryptographic properties and many functions based on it have been constructed [33,38–41,43]. We computed the transparency order of the Carlet–Feng function $CF \in \mathcal{B}_n$ [5], for $5 \leq n \leq 12$ and compared it with the upper bound given by Theorem 3.1 (see Table 4).

Rotation symmetric Boolean functions (RSBFs) We tested the transparency order for (7, 2, 4, 56) RSBFs. It is shown in [36] that there are 36 such functions with $f(0) = 0$. For these functions, $TO(f) = 1 - \frac{8}{127} = 0.937$, while the upper bound given by Theorem 3.1 is 0.992. It seems that the transparency order of such RSBFs is quite good compared to

functions with the same nonlinearity. The number of (8, 1, 6, 116) RSBFs with $f(0) = 0$ is precisely 10272. The truth table of an (8, 1, 6, 116) RSBF is given in [37] as follows

$$005562677d592d7a3be632c34da23bcc$$
$$0f8bfd3c5a49b05a31f6c94c5e9ae4a0,$$

which has quite a good transparency order, namely $TO(f) = 0.9618$. We recall that the lowest transparency order of balanced functions with the nonlinearity 116 found by [27] using the evolutionary computation methods is 0.962.

6 Transparency order and concatenations

There are quite a few constructions of functions with good cryptographic properties, which are concatenations of functions on fewer number of variables (more often than not, even affine functions). Consequently, we want to investigate how the transparency order of f compares with the transparency order of its components. To that effect, let $f \in \mathcal{B}_{n+1}$ and write $f(x, x_{n+1}) = f_1(x)||f_2(x)$, where $f_2 := f_1$ or $f_2 := \bar{f_1} = f_1 \oplus 1$.

Theorem 6.1 *Let $f_1, f_2 \in \mathcal{B}_n$ and $f(x, x_{n+1}) = f_1(x)||f_2(x)$. If $f_2 := f_1$ or $f_2 := \bar{f_1}$, then*

$$TO(f) = \frac{2^{n+1} - 2}{2^{n+1} - 1} TO(f_1).$$

In general,

$$TO(f) = 1 - \frac{2}{2^{n+1}(2^{n+1} - 1)} \left(2^n (2^n - 1)(1 - TO(f_1)) + \sum_{y \in \mathbb{F}_2^n} |\mathcal{C}_{f_1, f_2}(y)| \right).$$

Proof We shall show both claims at once, pointing out where we require $f_2 = f_1$, $f_2 = \bar{f_1}$. We first concentrate on the autocorrelation of f at (y, y_{n+1})

$$\begin{aligned} \mathcal{C}_f(y, y_{n+1}) &= \sum_{(x, x_{n+1}) \in \mathbb{F}_2^{n+1}} (-1)^{f(x, x_{n+1}) \oplus f(x \oplus y, x_{n+1} \oplus y_{n+1})} \\ &= \sum_{x_{n+1} = 0, x \in \mathbb{F}_2^n} (-1)^{f_1(x) \oplus \bar{y}_{n+1} f_1(x \oplus y) \oplus y_{n+1} f_2(x \oplus y)} \\ &\quad + \sum_{x_{n+1} = 1, x \in \mathbb{F}_2^n} (-1)^{f_2(x) \oplus y_{n+1} f_1(x \oplus y) \oplus \bar{y}_{n+1} f_2(x \oplus y)}. \end{aligned}$$

If $y_{n+1} = 0$, then

$$\begin{aligned} \mathcal{C}_f(y, 0) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f_1(x) \oplus f_1(x \oplus y)} + \sum_{x \in \mathbb{F}_2^n} (-1)^{f_2(x) \oplus f_2(x \oplus y)} \\ &= 2 \sum_{x \in \mathbb{F}_2^n} (-1)^{f_1(x) \oplus f_1(x \oplus y)} = 2 \mathcal{C}_{f_1}(y), \text{ if } f_2 = f_1 \text{ or } f_2 = \bar{f_1}. \end{aligned}$$

If $y_{n+1} = 1$, then

$$\begin{aligned}\mathcal{C}_f(y,1) &= \sum_{x\in\mathbb{F}_2^n} (-1)^{f_1(x)\oplus f_2(x\oplus y)} + \sum_{x\in\mathbb{F}_2^n} (-1)^{f_2(x)\oplus f_1(x\oplus y)} = 2\mathcal{C}_{f_1,f_2}(y)\\ &= 2\epsilon \sum_{x\in\mathbb{F}_2^n} (-1)^{f_1(x)\oplus f_1(x\oplus y)} = 2\epsilon\,\mathcal{C}_{f_1}(y), \text{ if } f_2 = f_1,\ f_2 = \bar{f_1},\end{aligned}$$

where $\epsilon = -1$ when $y_{n+1} = 1$ and $f_2 = \bar{f_1}$, and $\epsilon = 1$, otherwise.

Using this in the definition of the transparency order of f, and the identity $\sum_{y\neq 0} |\mathcal{C}_{f_1}(y)| = 2^n(2^n-1)(1-TO(f_1))$, we obtain

$$\begin{aligned}TO(f) &= 1 - \frac{1}{2^{n+1}(2^{n+1}-1)} \sum_{(y,y_{n+1})\neq 0} |\mathcal{C}_f(y,y_{n+1})|\\ &= 1 - \frac{1}{2^{n+1}(2^{n+1}-1)} \left(\sum_{y_{n+1}=0,\,y\neq 0} |\mathcal{C}_f(y,0)| + \sum_{y_{n+1}=1,\,y} |\mathcal{C}_f(y,1)| \right)\\ &= 1 - \frac{2}{2^{n+1}(2^{n+1}-1)} \left(\sum_{y\neq 0} |\mathcal{C}_{f_1}(y)| + \sum_{y} |\mathcal{C}_{f_1}(y)| \right), \text{ if } f_2 = f_1,\ f_2 = \bar{f_1}\\ &= 1 - \frac{2}{2^{n+1}(2^{n+1}-1)} \left(2^{n+1}(2^n-1)(1-TO(f_1)) + 2^n\right)\\ &= \frac{2^{n+1}-2}{2^{n+1}-1}\, TO(f_1),\end{aligned}$$

and both claims of the theorem are shown. □

7 Constructions of balanced semibent Boolean functions with provably relatively good transparency order

In this section, we will construct two infinite classes of n-variable balanced semibent Boolean functions with relatively good transparency order, where n is odd. The 5-variable function of the first class has the lowest transparency order among those 5-variable functions with the maximum nonlinearity 12. For $n \geq 9$, the n-variable function of the second class has lower transparency order than that of the first class.

Lemma 7.1 *Let $f = b_1||b_2$, where $b_1, b_2 \in \mathcal{B}_{n-1}$ are two bent functions. Then f is semibent and*

$$TO(f) = 1 - \frac{1}{2^{n-1}(2^n-1)} \sum_{y\in\mathbb{F}_2^{n-1}} \left| \sum_{x\in\mathbb{F}_2^{n-1}} (-1)^{b_1(x)\oplus b_2(x\oplus y)} \right|.$$

Particularly, if $b_1 = b_2$, then $TO(f) = 1 - \frac{1}{2^n-1}$, which is the same as the bound given by Theorem 6.1.

Proof It is well known that the concatenation of two bent functions is semibent. Let $y = (y_1, \ldots, y_n) \in \mathbb{F}_2^{n*}$. If $y_n = 0$, then

$$\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)\oplus f(x\oplus y)} = \sum_{\hat{x}\in\mathbb{F}_2^{n-1}}(-1)^{b_1(\hat{x})\oplus b_1(\hat{x}\oplus\hat{y})} \oplus \sum_{\hat{x}\in\mathbb{F}_2^{n-1}}(-1)^{b_2(\hat{x})\oplus b_2(\hat{x}\oplus\hat{y})} = 0,$$

where $\hat{y} = (y_1, \ldots, y_{n-1})$. If $y_n = 1$, then

$$\begin{aligned}\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)\oplus f(x\oplus y)} &= \sum_{\hat{x}\in\mathbb{F}_2^{n-1}}(-1)^{b_1(\hat{x})\oplus b_2(\hat{x}\oplus\hat{y})} \oplus \sum_{\hat{x}\in\mathbb{F}_2^{n-1}}(-1)^{b_2(\hat{x})\oplus b_1(\hat{x}\oplus\hat{y})}\\ &= 2\sum_{\hat{x}\in\mathbb{F}_2^{n-1}}(-1)^{b_1(\hat{x})\oplus b_2(\hat{x}\oplus\hat{y})},\end{aligned}$$

and the result follows. □

Theorem 7.2 *Let $F_1(x) = x_1x_2x_n \oplus x_1x_3x_n \oplus x_2x_4x_n \oplus x_3x_4x_n \oplus x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{n-2}x_{n-1} \oplus x_n$, where $n \geq 5$ is odd. Then F_1 is a balanced semibent function and*

$$TO(F_1) = 1 - \frac{2}{2^n - 1}.$$

Proof Clearly, $F_1 = b_3||b_4$, where $b_3(x) = x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{n-2}x_{n-1}$ and $b_4(x) = x_1x_3 \oplus x_2x_4 \oplus x_5x_6 \oplus \cdots \oplus x_{n-2}x_{n-1} \oplus 1$ are bent functions and $wt(b_3) + wt(b_4) = 2^{n-1}$. Therefore, F_1 is a balanced semibent function. Let $y = (y_1, \ldots, y_{n-1}) \in \mathbb{F}_2^{n-1}$. If there exists an $i > 4$ such that $y_i = 1$, then $b_3(x) \oplus b_4(x \oplus y) = x_{i-(-1)^i} \oplus h(x_1, \ldots, x_{i-(-1)^i-1}, x_{i-(-1)^i+1}, \ldots, x_{n-1})$ is balanced, where $h \in \mathcal{B}_{n-2}$. Now we consider the case $y = (y_1, y_2, y_3, y_4, 0, \ldots, 0)$. It is easy to check that $b_3(x) \oplus b_4(x \oplus y)$ is not balanced only when $(y_1, y_2, y_3, y_4) \in Y$, where $Y = \{(0,0,0,0), (0,1,1,0), (1,0,0,1), (1,1,1,1)\}$. Moreover, if $(y_1, y_2, y_3, y_4) \in Y$, then $x_1x_2 \oplus x_3x_4 \oplus (x_1 \oplus y_1)(x_3 \oplus y_3) \oplus (x_2 \oplus y_2)(x_4 \oplus y_4) \in \mathcal{B}_4$ is of weight 4 or 12. Therefore, by Lemma 7.1, we have

$$\begin{aligned}TO(F_1) &= 1 - \frac{1}{2^{n-1}(2^n-1)}\sum_{y\in\mathbb{F}_2^{n-1}}\left|\sum_{x\in\mathbb{F}_2^{n-1}}(-1)^{b_3(x)\oplus b_4(x\oplus y)}\right|\\ &= 1 - \frac{2^{n-5}}{2^{n-1}(2^n-1)}\sum_{y\in Y}\left|\sum_{x\in\mathbb{F}_2^4}(-1)^{x_1x_2\oplus x_3x_4\oplus(x_1\oplus y_1)(x_3\oplus y_3)\oplus(x_2\oplus y_2)(x_4\oplus y_4)}\right|\\ &= 1 - \frac{2^{n-5}}{2^{n-1}(2^n-1)}\cdot 4\cdot 8\\ &= 1 - \frac{2}{2^n-1},\end{aligned}$$

and the theorem is shown. □

Remark 7.3 By Lemma 7.1, the highest transparency order of an n-variable semibent function is $1 - \frac{1}{2^n-1}$. F_1 is a balanced semibent function with transparency order $1 - \frac{2}{2^n-1}$. Taking $n = 5$, we have $F_1(x) = x_1x_2x_5 \oplus x_1x_3x_5 \oplus x_2x_4x_5 \oplus x_3x_4x_5 \oplus x_1x_2 \oplus x_3x_4 \oplus x_5, nl(F_1) = 12$ and $TO(F_1) = 0.936$. From Table 1, F_1 has the lowest transparency order among those 5-variable Boolean functions with the nonlinearity 12. For general n, we do not know the lowest transparency order of n-variable semibent functions, which we leave as an open problem.

Theorem 7.4 *Let* $F_2(x) = (x_1x_2 \oplus x_1x_8 \oplus x_2x_7 \oplus x_3x_4 \oplus x_3x_6 \oplus x_4x_5 \oplus x_5x_6 \oplus x_7x_8)x_n \oplus x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{n-2}x_{n-1} \oplus x_n$, *where* $n \geq 9$ *is odd. Then* F_2 *is a balanced semibent function and*

$$TO(F_2) = 1 - \frac{4}{2^n - 1}.$$

Proof Clearly, $F_2 = b_5||b_6$, where $b_5(x) = x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{n-2}x_{n-1}$ and $b_6(x) = x_1x_8 \oplus x_2x_7 \oplus x_3x_6 \oplus x_4x_5 \oplus x_9x_{10} \cdots \oplus x_{n-2}x_{n-1} \oplus 1$ are bent functions and $wt(b_5) + wt(b_6) = 2^{n-1}$. Therefore, F_2 is a balanced semibent function. Similar to the proof of Theorem 7.2, we have

$$TO(F_2) = 1 - \frac{2^{n-9}}{2^{n-1}(2^n - 1)} \sum_{y \in \mathbb{F}_2^8} \left| \sum_{x \in \mathbb{F}_2^8} (-1)^{b_7(x) \oplus b_8(x \oplus y)} \right|,$$

where $b_7(x) = x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_7x_8$ and $b_8(x) = x_1x_8 \oplus x_2x_7 \oplus x_3x_6 \oplus x_4x_5$. Therefore,

$$TO(F_2) = 1 - \frac{2^{n-9}}{2^{n-1}(2^n - 1)} \cdot 16 \cdot 64,$$

and the result follows. □

Taking $n = 9$, we have $nl(F_2) = 240$ and $TO(F_2) = 0.992$. A natural question is whether F_2 has the lowest transparency order among those 9-variable balanced semibent functions. The answer is negative which can be seen from the following example.

Example 7.5 Let $F_3 = b_9||b_{10}$, where $b_9, b_{10} \in \mathcal{B}_8$, the truth table of b_9 is

$$555533330F0F00FF66665A5A55AA3C3C$$
$$33CC0FF0696966995AA53CC369960000$$

and the truth table of b_{10} is

$$BBF0BBC3AAB4994B883C880F66875578$$
$$FCA93065B7B7847BFC56309A847BB7B7.$$

It is easy to check that b_9, b_{10} are two Maiorana-McFarland functions [4,8] with degree 4, and F_3 is a balanced semibent function of degree 5. We have $TO(F_3) = 0.9745$, which is lower than that of F_2.

Remark 7.6 It is still an open problem whether there exist 8-variable balanced functions with nonlinearity 118. For 8-variable balanced functions with nonlinearity 116, using search algorithms, the lowest transparency order has been found is 0.958 [16]. Up until now, there exists no result on the transparency order of 9-variable Boolean functions. Example 7.5 provides a 9-variable balanced function with nonlinearity 240 and transparency order 0.9745. This value seems quite good, and it may be challenging to find 9-variable balanced functions with nonlinearity 240 and lower transparency order using search algorithms.

8 Conclusion

In this paper, we give some bounds between transparency order and nonlinearity, inferring the worst possible transparency order of those functions with the same nonlinearity. We

study certain classes of Boolean functions for their transparency order and find that the transparency order of some functions with low degree can be determined by their nonlinearity. Furthermore, we construct two infinite classes of balanced semibent Boolean functions with provably relatively good transparency order.

The field is still open and there are many problems deserving to be studied. To be specific, given some value of the nonlinearity, what is the minimum value of the transparency order? How do we construct highly nonlinear balanced functions with the minimum transparency order? The transparency order is a criterion for designing cryptographic algorithms to resist DPA attacks. We hope that our work would attract more researchers to be interested in this new and interesting notion.

Acknowledgements The authors would like to thank the reviewers of this manuscript for extraordinarily useful criticisms and suggestions. The first author would like to thank the financial support from the National Natural Science Foundation of China (Grant No. 61572189).

References

1. Bryant R.E.: On the complexity of VLSI implementations and graph representations of Boolean functions with application to integer multiplication. IEEE Trans. Comput. **40**(2), 205–213 (1991).
2. Canteaut A., Videau M.: Symmetric Boolean functions. IEEE Trans. Inf. Theory **51**, 2791–2811 (2005).
3. Carlet C.: On Highly Nonlinear S-Boxes and Their Inability to Thwart DPA Attacks. Progress in Cryptology-INDOCRYPT 2005, LNCS 3797, pp. 49–62. Springer, Berlin (2005).
4. Carlet C.: Boolean functions for cryptography and error correcting codes, chapter of the monography. In: Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 257–397. Cambridge University Press, Cambridge (2010). http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.
5. Carlet C., Feng K.: An Infinite Class of Balanced Functions with Optimal Algebraic Immunity, Good Immunity to Fast Algebraic Attacks and Good Nonlinearity. Advances in Cryptology-ASIACRYPT 2008, LNCS 5350, pp. 425–440. Springer, Berlin (2008).
6. Carlet C., Dalai D.K., Gupta K.C., Maitra S.: Algebraic immunity for cryptographically significant Boolean functions: analysis and construction. IEEE Trans. Inf. Theory **52**(7), 3105–3121 (2006).
7. Chakraborty K., Sarkar S., Maitra S., Mazumdar B., Mukhopadhyay D., Prouff E.: Redefining the transparency order. Des. Codes Cryptogr. **82**, 95–115 (2017).
8. Cusick T.W., Stănică P.: Cryptographic Boolean Functions and Applications, 2nd edn. Elsevier, Academic Press (2017).
9. Evci M.A., Kavut S.: DPA Resilience of Rotation-Symmetric S-boxes, IWSEC, pp. 146–157 (2014).
10. Fei Y., Luo Q., Ding A.A.: A Statistical Model for DPA with Novel Algorithmic Confusion Analysis, CHES 2012, LNCS 7428, pp. 233–250. Springer, Berlin (2012).
11. Fei Y., Ding A.A., Lao J., Zhang L.: A Statistics-Based Fundamental Model for Side-Channel Attack Analysis, IACR Cryptology ePrint Archive, Report 2014/152 (2014).
12. Feng K., Liao Q., Yang J.: Maximum values of generalized algebraic immunity. Des. Codes Cryptogr. **50**(2), 243–252 (2009).
13. Fischer W., Gammel B.M., Kniffler O., Velten J.: Differential Power Analysis of Stream Ciphers, CT-RSA 2007, LNCS 4377, pp. 257–270. Springer, Berlin (2006).
14. Guilley S., Pacalet R.: Differential Power Analysis Model and Some Results, CARDIS, pp. 127–142 (2004).
15. Harrison M.A.: On the classification of Boolean functions by the general linear and affine groups. J. Soc. Ind. Appl. Math. **12**(2), 285–299 (1964).
16. Jain A., Chaudhari N.S.: Evolving Highly Nonlinear Balanced Boolean Functions with Improved Resistance to DPA Attacks, NSS 2015, LNCS 9408, pp. 316–330. Springer, Berlin (2015).
17. Kocher P.: Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other systems, Advances in Cryptology–CRYPTO'96, LNCS 1109, pp. 104–113. Springer, Berlin (1996).
18. Kocher P., Jaffe J., Jun B.: Differential Power Analysis, Advances in Cryptology–CRYPTO'99, LNCS 1666, pp. 388–397. Springer, Berlin (1999).
19. Langevin P.: Classification of Boolean functions under the affine group. http://langevin.univ-tln.fr/project/agl/agl.html.

20. Maiorana J.A.: A classification of the cosets of the Reed–Muller code R(1,6). Math. Comput. **57**(195), 403–414 (1991).
21. Mangard S., Oswald E., Popp T.: Power Analysis Attacks-Revealing the Secrets of Smart Cards. Springer, Berlin (2007).
22. Mazumdar B., Mukhopadhyay D.: Construction of rotation symmetric *S*-boxes with high nonlinearity and improved DPA resistivity. IEEE Trans. Comput. **66**(1), 59–72 (2017).
23. Mazumdar B., Mukhopadhyay D., Sengupta I.: Design and implementation of rotation symmetric S-boxes with high nonlinearity and high DPA resilience. In: 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp. 87–92 (2013).
24. Mazumdar B., Mukhopadhyay D., Sengupta I.: Constrained search for a class of good bijective S-boxes with improved DPA resistivity. IEEE Trans. Inf. Forensics Secur. **8**(12), 2154–2163 (2013).
25. Nguyen C., Tran L., Nguyen K.: On the resistance of Serpent-type 4 bit S-boxes against differential power attacks, 2014 IEEE Fifth International Conference on Communication and Electronics (ICCE), pp. 542–547 (2014).
26. Patranabis S., Roy D.B., Chakraborty A., Nagar N., Singh A., Mukhopadhyay D., Ghosh S.: Lightweight design-for-security strategies for combined countermeasures against side channel and fault analysis in IoT applications. Journal of Hardware and Systems Security (to appear).
27. Picek S., Batina L., Jakobovic D.: Evolving DPA-Resistant Boolean Functions, PPSN 2014, LNCS 8672, pp. 812–821. Springer, Berlin (2014).
28. Picek S., Ege B., Batina L., Jakobovic D., Chmielewski L., Golub M.: On Using Genetic Algorithms for Intrinsic Side-channel Resistance: The Case of AES S-box. In: Proceedings of the First Workshop on Cryptography and Security in Computing Systems, ser. CS2, pp. 13–18 (2014).
29. Picek S., Ege B., Papagiannopoulos K., Batina L., Jakobovic D.: Optimality and beyond: the case of 4x4 S-boxes, 2014 In: IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp. 80–83 (2014).
30. Picek S., Papagiannopoulos K., Ege B., Batina L., Jakobovic D.: Confused by Confusion: Systematic Evaluation of DPA Resistance of Various S-boxes, Progress in Cryptology-INDOCRYPT 2014, LNCS 8885, pp. 374–390. Springer, Berlin (2014).
31. Picek S., Mazumdar B., Mukhopadhyay D., Batina L.: Modified Transparency Order Property: Solution or Just Another Attempt, SPACE 2015, LNCS 9354, pp. 210–227. Springer, Berlin (2015).
32. Prouff E.: DPA Attacks and S-Boxes, FSE 2005, LNCS 3557, pp. 424–441. Springer, Berlin (2005).
33. Rizomiliotis P.: On the resistance of boolean functions against algebraic attacks using univariate polynomial representation. IEEE Trans. Inf. Theory **56**(8), 4014–4024 (2010).
34. Sarkar S., Maitra S., Chakraborty K.: Differential Power Analysis in Hamming Weight Model: How to Choose among (Extended) Affine Equivalent S-boxes, Progress in Cryptology-INDOCRYPT 2014, LNCS 8885, pp. 360–373. Springer, Berlin (2014).
35. Selvam R., Shanmugam D., Annadurai S.: Decomposed *S*-Boxes and DPA Attacks: A Quantitative Case Study Using PRINCE, SPACE, pp. 179–193 (2016).
36. Stănică P., Maitra S.: Rotation symmetric boolean functions-count and cryptographic properties. Discret. Appl. Math. **156**, 1567–1580 (2008).
37. Stănică P., Maitra S., Clark J.: Results on rotation symmetric bent and correlation immune Boolean functions, FSE 2004, LNCS 3017, pp. 161–177. Springer, Berlin (2004)
38. Tan C., Goh S.: Several classes of even-variable balanced Boolean functions with optimal algebraic immunity. IEICE Trans. **E94.A**(1), 165–171 (2011).
39. Tang D., Carlet C., Tang X.: Highly nonlinear boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks. IEEE Trans. Inf. Theory **59**(1), 653–664 (2013).
40. Tu Z., Deng Y.: A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity. Des. Codes Cryptogr. **60**(1), 1–14 (2011).
41. Wang Q., Peng J., Kan H., Xue X.: Constructions of cryptographically significant Boolean functions using primitive polynomials. IEEE Trans. Inf. Theory **56**(6), 3048–3053 (2010).
42. Wang Q., Carlet C., Stănică P., Tan C.: Cryptographic properties of the hidden weighted bit function. Discret. Appl. Math. **174**, 1–10 (2014).
43. Zeng X., Carlet C., Shan J., Hu L.: More balanced Boolean functions with optimal algebraic immunity, and good nonlinearity and resistance to fast algebraic attacks. IEEE Trans. Inf. Theory **57**(9), 6310–6320 (2011).