Construction of n-variable ($n \equiv 2 \bmod 4$) balanced Boolean functions with maximum absolute value in autocorrelation spectra $< 2^{\frac{n}{2}}$

Deng Tang and Subhamoy Maitra

Abstract

In this paper we consider the maximum absolute value Δ_f in the autocorrelation spectrum (not considering the zero point) of a function f. In even number of variables n, bent functions possess the highest nonlinearity with $\Delta_f = 0$. The long standing open question (for two decades) in this area is to obtain a theoretical construction of balanced functions with $\Delta_f < 2^{\frac{n}{2}}$. So far there are only a few examples of such functions for $n = 10, 14$, but no general construction technique is known. In this paper, we mathematically construct an infinite class of balanced Boolean functions on n variables having absolute indicator strictly lesser than $\delta_n = 2^{\frac{n}{2}} - 2^{\frac{n+6}{4}}$, nonlinearity strictly greater than $\rho_n = 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-3} - 5 \cdot 2^{\frac{n-2}{4}}$ and algebraic degree $n-1$, where $n \equiv 2 \pmod 4$ and $n \geq 46$. While the bound $n \geq 46$ is required for proving the generic result, our construction starts from $n = 18$ and we could obtain balanced functions with $\Delta_f < 2^{\frac{n}{2}}$ and nonlinearity $> 2^{n-1} - 2^{\frac{n}{2}}$ for $n = 18, 22$ and 26.

Index Terms

Absolute Indicator, Autocorrelation Spectrum, Balancedness, Boolean function, Nonlinearity.

I. Introduction

Symmetric-key cryptography, which includes stream ciphers and block ciphers, plays a very important role in modern cryptography. The fundamental and generally accepted design principles for symmetric-key cryptography are *confusion* and *diffusion*, introduced by Shannon [23]. Confusion means making the relation between the ciphertext and the plaintext as complex as possible for the attacker and diffusion is the spreading out of the influence of one or several arbitrary bits of the plaintext or/and of the key over the output bits. These two design principles are very general and informal, but while considering a Boolean function as a primitive of a cipher design, confusion relates to Walsh spectrum and diffusion relates to autocorrelation spectrum of the said Boolean function. The motivation of a good cryptographic design is to minimize the maximum absolute values in both the spectra.

In this direction, there are several long standing open questions in the domain of Boolean functions. For even number of variables n, the two main conjectures related to balanced Boolean functions are as follows:

- 1994: $nlb(n) \leq 2^{n-1} - 2^{\frac{n}{2}} + nlb(\frac{n}{2})$ [6], where $nlb(n)$ is maximum nonlinearity of balanced Boolean functions on n variables;
- 1996: $\Delta_f \geq 2^{\frac{n}{2}}$ [27].

While the first one is still standing, the second one has been disproved for a few cases namely $n = 10, 14$ and each of those had been considered to be important milestone in Boolean function research (see Table I). Such functions could be achieved by heuristic search. In this paper, two decades after the conjecture [27] had been placed, we could provide a specific construction method to discover an infinite class of such functions. Our construction is possible for $n \geq 18$, though our generic proof for $\Delta_f < 2^{\frac{n}{2}}$ starts from $n \geq 46$.

In even number of variables, it is well-known that bent functions [19] possess the highest nonlinearity and all the nonzero values in its autocorrelation spectrum is zero. Unfortunately, bent functions are not balanced and not generally used directly in the design of symmetric-key cryptography. Therefore, the main challenge for the construction of balanced highly nonlinear Boolean functions f in even number of variables n is to obtain very low absolute indicator Δ_f. With respect to this challenge, Zhang and Zheng proposed the following Conjecture.

D. Tang is with School of Mathematics, Southwest Jiaotong University, Chengdu 610031, China and Science and Technology on Communication Security Laboratory, Chengdu 610041, China. Email: dtang@foxmail.com

S. Maitra is with the Applied Statistics Unit, Indian Statistical Institute, 203 B. T. Road, Kolkata 700108, India. E-mail: subho@isical.ac.in

Conjecture 1 ([27], Conjecture 1)**.** *The absolute indicator of any balanced Boolean function f of algebraic degree no less than 3 is lower-bounded by $2^{\lfloor \frac{n+1}{2} \rfloor}$.*

For odd variables n, this conjecture has been disproved for $n = 9, 11$ in [7], $n = 15$ in [15] and $n = 21$ in [14], [10]. Till date, for even n, this conjecture has been disproved only for $n = 10$ [7] and 14 [1]. That is, there is no evidence that there are balanced Boolean functions with absolute indicator strictly less than $2^{\frac{n}{2}}$ for an infinite class. Note that the integers 10 and 14 are $2 \pmod 4$ as we construct for a general class in this paper.

TABLE I
BALANCED FUNCTIONS $f \in \mathcal{B}_n$ ($n \equiv 2 \bmod 4$) WITH $\Delta_f < 2^{\frac{n}{2}}$

Results	n	Δ_f	Degree	Nonlinearity
S. Kavut *et al.* [7]	10	24	9	488
L. Burnett *et al.* [1]	14	104	13	8102
	14	112	13	8104
Construction 1 (example)	18	480 ($\delta_n = 448, \delta'_n = 512$)	17	130664 ($\rho_n = 130544, \rho'_n = 130560$)
Construction 1 (example)	22	1880 ($\delta_n = 1920, \delta'_n = 2048$)	21	2095484 ($\rho_n = 2095200, \rho'_n = 2095104$)
Construction 1 (example)	26	7856 ($\delta_n = 7936, \delta'_n = 8192$)	25	33547436 ($\rho_n = 33546944, \rho'_n = 33946240$)
Construction 1 (theory)	≥ 46	$< \delta_n$	$n-1$	$> \rho_n$

Here, $\rho_n = 2^{n-1} - 7 \cdot 2^{\frac{n}{2}-3} - 5 \cdot 2^{\frac{n-2}{4}} = 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-3} - 5 \cdot 2^{\frac{n-2}{4}}$, $\rho'_n = 2^{n-1} - 2^{\frac{n}{2}}$, $\delta_n = 2^{\frac{n}{2}} - 2^{\frac{n+6}{4}}$ and $\delta'_n = 2^{\frac{n}{2}}$. The implications of these values are important for our examples corresponding to $n = 18, 22, 26$ as in these cases our construction works, but our theoretical results can take care of the cases only for $n \geq 46$.

In the present paper, we propose a method for constructing balanced Boolean functions in even number of variables with very low absolute indicator and strictly almost optimal nonlinearity. Our construction base on a modification of the simplest partial spread ($\mathcal{PS}$) bent function in n variables, in which the $\mathcal{PS}$ bent function was introduced by Dillon [4] in his PhD thesis. As a result, we can obtain an infinite class of balanced Boolean functions f in n variables with absolute indicator strictly lesser than $2^{\frac{n}{2}} - 2^{\frac{n+6}{4}}$, nonlinearity strictly greater than $2^{n-1} - 7 \cdot 2^{\frac{n}{2}-3} - 5 \cdot 2^{\frac{n-2}{4}}$ and algebraic degree $n-1$, where $n \equiv 2 \pmod 4$ and $n \geq 46$. This is the first time that an infinite class of balanced Boolean functions with absolute indicator strictly lesser than $2^{\frac{n}{2}}$ have been exhibited, which can be also viewed as an infinite class of counterexamples against Conjecture 1.

We like to underline that the construction that we present here requires substantially involved as well as tricky ideas. For a quick look, the broad steps are as follows.

- Lemma 3: g_0, g_1 are two specially constructed Boolean functions on 4 variables.
- Lemma 4: Two quadratic bent functions s_0, s_1 on $(t-1)$ variables where $t \geq 5$ is odd, with certain properties that provide two functions w_0, w_1 on t variables.
- Definition 3 and Lemma 6: Construction of h_0 (based on g_0, w_0) and h_1 (based on g_1, h_1), on $k = t + 4$ variables, i.e., $k \geq 9$ odd.
- Construction 1: A bent function on $n = 2k$ variables is modified using the two k-variable functions h_0, h_1 to obtain an n-variable balanced function f. As k is odd, n is $2 \bmod 4$.
- Theorem 1: The proof that $\Delta_f < 2^{\frac{n}{2}}$ for $n \geq 46$.
- Example 1: The lowest number of variables, on which this construction is possible, is $n = 2k = 18$. This n is not covered by Theorem 1. However, we checked this balanced function f by computer program to note that $\Delta_f = 480 < 2^{\frac{18}{2}}$. This works for $n = 22, 26$ too.
- Theorems 2 and 3: Results explaining the nonlinearity and algebraic degree respectively.

The rest of this paper is organized as follows. In Section II, necessary background is reviewed. Then, in Section III, we explain two preliminary functions that will be used towards the main construction. Our construction and main results are presented in Section IV. Finally, Section V concludes the paper.

II. PRELIMINARIES

Let $\mathbb{F}_2^n$ be the vector space of n-tuples over the field $\mathbb{F}_2$ of two elements. For any positive integer n, we shall denote by $\mathbf{0}$ (respectively $\mathbf{1}$) the all-zero vector (respectively all-one vector) of $\mathbb{F}_2^n$. A *Boolean function* on n

variables is a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. Denote by $\mathcal{B}_n$ the set of all the 2^{2^n} Boolean functions of n variables. The basic representation of an n-variable Boolean function f is by its *truth table*, *i.e.*,

$$f = \big[f(0,0,\cdots,0), f(1,0,\cdots,0), \cdots, f(1,1,\cdots,1)\big].$$

The *support* of f, denoted by $\mathrm{supp}(f)$, is defined as the set $\{x \in \mathbb{F}_2^n \,|\, f(x) \neq 0\}$. The *Hamming weight* of f, denoted by $\mathrm{wt}(f)$, is defined as the Hamming weight of the truth table of f, or in other words, the size of the support of f. We say that the Boolean function $f \in \mathcal{B}_n$ is *balanced* if its Hamming weight equals 2^{n-1}. It is well-known that any Boolean function $f \in \mathcal{B}_n$ can be uniquely represented by a multivariate polynomial over $\mathbb{F}_2$, called the *algebraic normal form* (ANF), in the form:

$$f(x_1, \cdots, x_n) = \bigoplus_{u \in \mathbb{F}_2^n} a_u \Big(\prod_{j=1}^{n} x_j^{u_j}\Big),$$

where $a_u \in \mathbb{F}_2$ and $u = (u_1, \cdots, u_n)$. The *algebraic degree*, denoted by $\deg(f)$, is the maximal value of $\mathrm{wt}(u)$ such that $a_u \neq 0$. A Boolean function is an *affine function* if its algebraic degree is at most 1. The set of all affine functions is denoted by A_n. In order to resist the Berlekamp-Massey algorithm [16], [20] and the Rønjom-Helleseth attack [18], Boolean functions used in stream ciphers should have high algebraic degree. It should be noted that the maximum algebraic degree of a balanced Boolean function of n variables is $n-1$.

Note that the vector space $\mathbb{F}_2^n$ is isomorphic to the finite field $\mathbb{F}_{2^n}$ through the choice of some basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. If $(\lambda_1, \lambda_2, \cdots, \lambda_n)$ is a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, then every vector $x = (x_1, \cdots, x_n)$ of $\mathbb{F}_2^n$ can be identified with the element $x_1\lambda_1 + x_2\lambda_2 + \cdots + x_n\lambda_n \in \mathbb{F}_{2^n}$. The finite field $\mathbb{F}_{2^n}$ can then be viewed as an n-dimensional vector space over $\mathbb{F}_2$. Further, each of its elements can be identified with a binary vector of length n and clearly the element $0 \in \mathbb{F}_{2^n}$ is identified with the all-zero vector. In the rest of this paper, we shall still use x to denote this element of the finite field. Thus, any Boolean function in n variables can be defined over $\mathbb{F}_{2^n}$ and uniquely expressed by an *univariate polynomial*

$$f(x) = \sum_{i=0}^{2^n-1} f_i x^i,$$

where $f_0, f_{2^n-1} \in \mathbb{F}_2$, $f_i \in \mathbb{F}_{2^n}$ is such that $f_{2i\,[\mathrm{mod}\ 2^n-1]} = f_i^2$ for $1 \leq i < 2^n - 1$. The algebraic degree under this representation $\deg(f)$ is equal to $\max\{\mathrm{wt}(\bar{i}) \,|\, f_i \neq 0, 0 \leq i < 2^n\}$, where $\bar{i}$ is the *binary expansion* of i. It is well-known that $\mathbb{F}_2^n$ can be written as $\mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2}$ when n is even. Recall that the vector space $\mathbb{F}_2^{n/2}$ is isomorphic to the finite field $\mathbb{F}_{2^{n/2}}$ through the choice of some basis of $\mathbb{F}_{2^{n/2}}$ over $\mathbb{F}_2$. Thus, the finite field $\mathbb{F}_{2^n}$ can be viewed as $\mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}} = \mathbb{F}_{2^{n/2}}^2$. Hence, any Boolean function in even number of n variables can be viewed over $\mathbb{F}_{2^{n/2}}^2$ and uniquely expressed by a *bivariate polynomial*

$$f(x,y) = \sum_{i,j=0}^{2^{n/2}-1} f_{i,j} x^i y^j,$$

where $f_{i,j} \in \mathbb{F}_{2^{n/2}}$ is such that

- $f_{2i\,[\mathrm{mod}\ 2^{n/2}-1], 2j\,[\mathrm{mod}\ 2^{n/2}-1]} = f_{i,j}^2$,
- $f_{2^{n/2}-1, 2j\,[\mathrm{mod}\ 2^{n/2}-1]} = f_{2^{n/2}-1,j}^2$, and
- $f_{2i\,[\mathrm{mod}\ 2^{n/2}-1], 2^{n/2}-1} = f_{i,2^{n/2}-1}^2$,

for $0 \leq i,j < 2^{n/2} - 1$. The algebraic degree $\deg(f)$ equals $\max\{\mathrm{wt}(\bar{i}) + \mathrm{wt}(\bar{j}) \,|\, f_{i,j} \neq 0\}$.

The *rth-order nonlinearity* of a Boolean function $f \in \mathcal{B}_n$ is defined as its minimum Hamming distance from f to all the n-variable Boolean functions of degree at most r

$$\mathrm{nl}_r(f) = \min_{g \in \mathcal{B}_n,\, \deg(g) \leq r} (d_H(f,g)),$$

where $d_H(f,g)$ is the Hamming distance between f and g, *i.e.*, $d_H(f,g) = |\{x \in \mathbb{F}_2^n \,|\, f(x) \neq g(x)\}|$. The first-order nonlinearity of f is simply called the *nonlinearity* of f and is denoted by $\mathrm{nl}(f)$. The nonlinearity $\mathrm{nl}(f)$ is the minimum Hamming distance between f and all the affine functions. In order to resist the best affine approximation [5] and the fast correlation attack [17], Boolean functions used in a cryptosystem must have high nonlinearity.

Definition 1. *In the present paper, a Boolean function in n variables is called to have* strictly almost optimal nonlinearity *if its nonlinearity is strictly greater than $2^{n-1} - 2^{\lceil \frac{n}{2} \rceil}$.*

The nonlinearity can also be expressed by means of the Walsh transform of f. Let $x = (x_1, x_2, \cdots, x_n)$ and $\omega = (\omega_1, \omega_2, \cdots, \omega_n)$ both belong to $\mathbb{F}_2^n$ and let $x \cdot \omega$ be the usual inner product in $\mathbb{F}_2^n$, then the Walsh transform of $f \in \mathcal{B}_n$ at point ω is defined by

$$W_f(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + \omega \cdot x}.$$

The multiset constituted by the values of the Walsh transform is called the *Walsh spectrum* of f. Over $\mathbb{F}_{2^n}$, the Walsh transform of f at point a can be defined by

$$W_f(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + \mathrm{Tr}_1^n(ax)},$$

where $\mathrm{Tr}_1^n(x) = \sum\limits_{i=0}^{n-1} x^{2^i}$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Over $\mathbb{F}_{2^{n/2}}^2$, the Walsh transform of f at point $(a, b) \in \mathbb{F}_{2^{n/2}}^2$ can be defined as

$$W_f(a, b) = \sum_{x, y \in \mathbb{F}_{2^{n/2}}} (-1)^{f(x,y) + \mathrm{Tr}_1^k(ax + by)},$$

where $a, b \in \mathbb{F}_{2^{n/2}}$. Then, the nonlinearity of a Boolean function $f \in \mathcal{B}_n$ can be computed as

$$\begin{aligned} \mathrm{nl}(f) &= 2^{n-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)| \\ &= 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}} |W_f(a)| \\ &= 2^{n-1} - \frac{1}{2} \max_{a, b \in \mathbb{F}_{2^{n/2}}} |W_f(a, b)| \quad \text{if } n \text{ even.} \end{aligned}$$

The well-known Parseval's relation [12] states that: for any n-variable Boolean function, we have $\sum_{u \in \mathbb{F}_2^n} {W_f}^2(u) = 2^{2n}$. Parseval's relation implies that, for a Boolean function of n variables, the mean of square of Walsh spectrum equals 2^n. Then the maximum of the square of Walsh spectrum is greater than or equal to 2^n and therefore $\max_{u \in \mathbb{F}_2^n} |W_f(u)| \geq 2^{\frac{n}{2}}$. This implies that the nonlinearity $\mathrm{nl}(f)$ is upper-bounded by $2^{n-1} - 2^{\frac{n}{2}-1}$. This upper bound $2^{n-1} - 2^{\frac{n}{2}-1}$ is tight for even n. The functions achieving the equality are called *bent* [19]. Bent functions are interesting combinatorial objects with the important property of having the maximum Hamming distance to the set of all affine functions. Bent functions are not balanced and their algebraic degrees are upper-bounded by $\frac{n}{2}$. Thus they are generally not suitable for direct cryptographic use.

To provide the property of diffusion to the cryptosystems, it is desirable for functions used in symmetric-key cryptography to have low autocorrelation. The autocorrelation function of a Boolean function f at a point α is defined by

$$C_f(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + f(x + \alpha)}.$$

In 1985, Webster and Tavares [26] introduced the concept of strict avalanche criterion (SAC) when searching for principles for designing DES-like data encryption algorithms. A Boolean function $f \in \mathcal{B}_n$ is said to satisfy strict avalanche criterion (SAC) if

$$C_f(\alpha) = 0 \text{ for all } \mathrm{wt}(\alpha) = 1.$$

In 1995, Zhang and Zheng [27] pointed out that SAC is a measure for local avalanche and hence has some limitations. So, they proposed the global avalanche characteristics (GAC).

Definition 2. *Let f be an arbitrary Boolean function in n variables. The global avalanche characteristics (GAC) of f is related to two indicators: the absolute indicator*

$$\Delta_f = \max_{\alpha \neq \boldsymbol{0}} |C_f(\alpha)|$$

and the sum-of-squares indicator

$$\sigma_f = \sum_{\alpha \in \mathbb{F}_2^n} C_f^2(\alpha).$$

Lemma 1. *([19]) A Boolean function $f \in \mathcal{B}_n$ is bent if and only if $C_f(\omega) = 0$ for any $\omega \in \mathbb{F}_2^{n*}$.*

Given a bent function f, by $\tilde{f}$ we denote the dual of that function, which is also bent.

Lemma 2. *Let $f_1, f_2 \in \mathcal{B}_n$ be two bent functions such that $\tilde{f_1} + \tilde{f_2}$ is also a bent function. Then for any $a \in \mathbb{F}_2^n$ we have $\sum_{x \in \mathbb{F}_2^n} (-1)^{f_1(x)+f_2(x+a)} \in \{2^{\frac{n}{2}}, -2^{\frac{n}{2}}\}$.*

Proof. It follows from [21, Corollary 3.3] that

$$\begin{aligned}
\sum_{x \in \mathbb{F}_2^n} (-1)^{f_1(x)+f_2(x+a)} &= 2^{-n} \sum_{u \in \mathbb{F}_2^n} W_{f_1}(u) \Big(\sum_{x \in \mathbb{F}_2^n} (-1)^{f_2(x+a)+u \cdot x} \Big) \\
&= 2^{-n} \sum_{u \in \mathbb{F}_2^n} W_{f_1}(u) W_{f_2}(u) (-1)^{u \cdot a} \\
&= \sum_{u \in \mathbb{F}_2^n} (-1)^{\tilde{f_1}(u)+\tilde{f_2}(u)+u \cdot a} \\
&\in \{2^{\frac{n}{2}}, -2^{\frac{n}{2}}\}
\end{aligned}$$

This completes the proof. □

III. Two preliminary functions for main construction

In this section, we present two classes of Boolean functions, denoted by h_0 and h_1 respectively, which will be employed in the main construction (see Construction 1 below) of this paper. We first present two Boolean functions g_0, g_1 in four variables, which will be useful in the design of h_0, h_1, and their cryptographic properties.

Lemma 3. *Let g_0, g_1 be two Boolean functions in four variables and their truth tables are given as follows:*

- $g_0 = [0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0]$*;*
- $g_1 = [1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1]$.

The following properties of g_0 and g_1 can be checked:

1) $\mathrm{wt}(g_0) + \mathrm{wt}(g_1) = 16$*;*
2) $\deg(g_0) = \deg(g_1) = 3$*;*
3) $\mathrm{nl}(g_0) = \mathrm{nl}(g_1) = 2$*;*
4) $C_{g_0}(\beta), C_{g_1}(\beta) \in \{8, 16\}$ *for any $\beta \in \mathbb{F}_2^4$;*
5) $C_{g_0}(\beta) + C_{g_1}(\beta) \in \{16, 24\}$*, for any $\beta \in \mathbb{F}_2^{4^*}$ where $\mathbb{F}_2^{4^*} = \mathbb{F}_2^4 \setminus \{\mathbf{0}\}$;*
6) $2 \sum_{y \in \mathbb{F}_2^4} (-1)^{g_0(y)+g_1(y+\beta)} \in \{-16, -24\}$*, for any $\beta \in \mathbb{F}_2^4$.*

Lemma 4. *Let $t \geq 5$ be an odd number. Let $s_0(y_1, \cdots, y_{t-1})$ and $s_1(y_1, \cdots, y_{t-1})$ be two quadratic bent functions on $\mathbb{F}_2^{t-1}$ such that $\mathrm{wt}(s_0) = \mathrm{wt}(s_1) = 2^{t-2} - 2^{(t-1)/2-1}$ and $\tilde{s_0} + \tilde{s_1}$ is a bent function as well. Define two Boolean functions w_0, w_1 on $\mathbb{F}_2^t$ as $w_0(y_1, \cdots, y_t) = y_t s_0$ and $w_1(y_1, \cdots, y_t) = y_t s_1$. Then the following statements hold:*

1) $\sum_{y \in \mathbb{F}_2^t} (-1)^{w_0(y)+w_1(y+\beta)} \in \{2^{t-1} \pm 2^{(t-1)/2}, 2^{(t+1)/2}\}$ *for any $\beta = (\beta_1, \cdots, \beta_t) \in \mathbb{F}_2^t$;*
2) $C_{w_0}(\beta) = C_{w_1}(\beta) = \begin{cases} 2^t, & \text{if } \beta = \mathbf{0} \\ 2^{t-1}, & \text{if } \beta_t = 0, \\ 2^{(t+1)/2}, & \text{if } \beta_t = 1 \end{cases}$ *for any $\beta = (\beta_1, \cdots, \beta_t) \in \mathbb{F}_2^{t^*}$;*
3) $|W_{w_0}(\beta)| = |W_{w_1}(\beta)| = \begin{cases} 2^{t-1} + 2^{(t-1)/2}, & \text{if } \beta = \mathbf{0} \\ 2^{t-1} - 2^{(t-1)/2}, & \text{if } \beta = (0, \cdots, 0, 1) \\ 2^{(t-1)/2}, & \text{if } \beta \in \mathbb{F}_2^{t^*} \setminus \{(0, \cdots, 0, 1)\} \end{cases}$.

Proof. For any $\beta = (\beta_1, \beta_2, \cdots, \beta_t) \in \mathbb{F}_2^t$, we define $\beta' = (\beta_1, \beta_2, \cdots, \beta_{t-1})$, *i.e.*, $\beta = (\beta', \beta_t)$.

1) Note that for any $(\beta', \beta_t), (y', y_t) \in \mathbb{F}_2^t$ we have $w_1(y + \beta) = (\beta_t + y_t) s_1(\beta' + y')$. Thus, we immediately get that $\sum_{y \in \mathbb{F}_2^t} (-1)^{w_0(y)+w_1(y+\beta)} = 2^{t-1} + \sum_{y' \in \mathbb{F}_2^{t-1}} (-1)^{s_0(y')+s_1(y'+\beta')}$ if $\beta_t = 0$, which is equal to $2^{t-1} \pm$

$2^{(t-1)/2}$ according to Lemma 2. If $\beta_t = 1$, we have $\sum_{y\in\mathbb{F}_2^t}(-1)^{w_0(y)+w_1(y+\beta)} = \sum_{y'\in\mathbb{F}_2^{t-1}}(-1)^{0+s_1(y'+\beta')} + \sum_{y'\in\mathbb{F}_2^{t-1}}(-1)^{s_0(y')+0} = 2^{(t+1)/2}$. Therefore, we have $\sum_{y\in\mathbb{F}_2^t}(-1)^{w_0(y)+w_1(y+\beta)} \in \{2^{t-1} \pm 2^{(t-1)/2}, 2^{(t+1)/2}\}$ for any $\beta \in \mathbb{F}_2^t$.

2) Clearly, we have $C_{w_0}(\beta) = C_{w_1}(\beta) = 2^t$ when $\beta = \mathbf{0}$. Note again that $w_1(y+\beta) = (\beta_t + y_t)s_1(\beta' + y')$. So for $\beta_t = 0$ we have $C_{w_1}(\beta) = \sum_{y'\in\mathbb{F}_2^{t-1}}(-1)^{0+0} + \sum_{y'\in\mathbb{F}_2^{t-1}}(-1)^{s_1(y')+s_1(y'+\beta')} = 2^{t-1}$ by Lemma 1, and we have $C_{w_1}(\beta) = \sum_{y'\in\mathbb{F}_2^{t-1}}(-1)^{0+s_1(y'+\beta')} + \sum_{y'\in\mathbb{F}_2^{t-1}}(-1)^{s_1(y')+0} = 2\sum_{y'\in\mathbb{F}_2^{t-1}}(-1)^{s_1(y')} = 2^{(t+1)/2}$ if $\beta_t = 1$. Similarly, we can get the values of $C_{w_0}(\beta)$ for all $\beta \in \mathbb{F}_2^t$.

3) Note that for any $\beta = (\beta', \beta_t) \in \mathbb{F}_2^t$ we have $W_{w_1}(\beta) = \sum_{y\in\mathbb{F}_2^t}(-1)^{w_1(y)+\beta\cdot y} = \sum_{y\in\mathbb{F}_2^t}(-1)^{y_t s_1(y')+\beta'\cdot y'+y_t\beta_t} = \sum_{(y',0)\in\mathbb{F}_2^{t-1}\times\{0\}}(-1)^{\beta'\cdot y'} + \sum_{(y',1)\in\mathbb{F}_2^{t-1}\times\{1\}}(-1)^{s_1(y')+\beta'\cdot y'+\beta_t}$. Recall that s_1 is a bent function and note that $\sum_{y'\in\mathbb{F}_2^{t-1}}(-1)^{\beta'\cdot y'} = 2^{t-1}$ if $\beta' = \mathbf{0}'$ and equals 0 otherwise. So we can immediately get that $W_{w_1}(\beta) = 2^{t-1} + 2^{(t-1)/2}$ if $\beta = \mathbf{0}$, $W_{w_1}(\beta) = 2^{t-1} - 2^{(t-1)/2}$ if $\beta = (0, \cdots, 0, 1)$, and $W_{w_1}(\beta) = 2^{(t-1)/2}$ if $\beta \in \mathbb{F}_2^{t^*} \backslash \{(0, \cdots, 0, 1)\}$. Similarly, we can get the values of $W_{w_0}(\beta)$ for all $\beta \in \mathbb{F}_2^t$. □

We are now ready to present the construction of h_0 and h_1.

Definition 3. *Let $k \geq 9$ be an odd integer. The two Boolean functions h_0 and h_1 in k variables defined as follows:*

- $h_0(y_1, \cdots, y_k) = g_0(y') + w_0(y'')$
- $h_1(y_1, \cdots, y_k) = g_1(y') + w_1(y'')$

where $y' = (y_1, y_2, y_3, y_4) \in \mathbb{F}_2^4, y'' = (y_5, y_6, \cdots, y_k) \in \mathbb{F}_2^{k-4}$, $g_0, g_1 \in \mathcal{B}_4$ defined by Lemma 3 and $w_0, w_1 \in \mathcal{B}_{k-4}$ defined by Lemma 4.

It is noted that the form of function h_0 (resp. h_1) is called the direct sum of Boolean functions w_0 and g_0 (resp. w_1 and g_1). We shall now provide the cryptographic properties of Boolean functions h_0 and h_1. For doing this, we first need the following lemma on direct sum of two Boolean functions.

Lemma 5 ([22]). *Let three positive integers k, r and e such that $k = r + e$. Let $h(y_1, \cdots, y_k) = g(y_1, \cdots, y_r) + s(y_{r+1}, \cdots, y_k)$, where $g \in \mathcal{B}_r$ and $s \in \mathcal{B}_e$. For any $\beta \in \mathbb{F}_2^k$, we have*

1) $W_h(\beta) = W_g(\beta') \cdot W_s(\beta'')$
2) $C_h(\beta) = C_g(\beta') \cdot C_s(\beta'')$

where $\beta = (\beta', \beta'') \in \mathbb{F}_2^4 \times \mathbb{F}_2^{k-4}$ with $\beta' = (\beta_1, \cdots, \beta_r)$ and $\beta'' = (\beta_{r+1}, \cdots, \beta_k)$.

Lemma 6. *Let $k \geq 9$ be an odd integer and h_0, h_1 be two Boolean functions in k variables defined by Definition 3. Then the following statements hold:*

1) $\deg(h_0) = \deg(h_1) = 3$;
2) $2^{(k+5)/2} \leq C_{h_0}(\beta) + C_{h_1}(\beta) \leq 3 \cdot 2^{k-1}$ *for any* $\beta \in \mathbb{F}_2^{k^*}$;
3) $-3 \cdot 2^{k-2} - 3 \cdot 2^{(k+1)/2} \leq 2\sum_{y\in\mathbb{F}_2^k}(-1)^{h_0(y)+h_1(y+\beta)} \leq -2^{(k+5)/2}$ *for any* $\beta \in \mathbb{F}_2^k$;
4) $|\max_{\beta\in\mathbb{F}_2^k} W_{h_0}(\beta)| = |\max_{\beta\in\mathbb{F}_2^k} W_{h_1}(\beta)| = |\max_{\beta'\in\mathbb{F}_2^4} W_{g_0}(\beta')| \cdot |\max_{\beta''\in\mathbb{F}_2^{k-4}} W_{w_0}(\beta'')|$
$= |\max_{\beta'\in\mathbb{F}_2^4} W_{g_1}(\beta')| \cdot |\max_{\beta''\in\mathbb{F}_2^{k-4}} W_{w_1}(\beta'')| = 3 \cdot 2^{k-3} + 3 \cdot 2^{(k-1)/2}$;
5) $\mathrm{wt}(h_0) + \mathrm{wt}(h_1) = 2^k$.

Proof. It can be easily seen that the algebraic degrees of h_0 and h_1 are equal to 3 since $\deg(g_0) = \deg(g_0) = 3$ and $\deg(w_0) = \deg(w_0) = 3$. In what follows, we prove the Items 2, 3, 4 respectively.

2) For any $\beta = (\beta', \beta'') \in \mathbb{F}_2^4 \times \mathbb{F}_2^{k-4}$, it follows from Lemma 5 that $C_{h_0}(\beta) + C_{h_1}(\beta) = C_{g_0}(\beta') \cdot C_{w_0}(\beta'') + C_{g_1}(\beta') \cdot C_{w_1}(\beta'')$. Note that $C_{g_0}(\mathbf{0}') = C_{g_1}(\mathbf{0}') = 2^4$ and $C_{w_0}(\mathbf{0}'') = C_{w_1}(\mathbf{0}'') = 2^{k-4}$. Then by Item 5) of Lemma 3 and Item 2) of Lemma 4 we arrive at $2^{(k+5)/2} \leq C_{h_0}(\beta) + C_{h_1}(\beta) \leq 3 \cdot 2^{k-1}$ for any $\beta \in \mathbb{F}_2^{k^*}$.

3) For any $\beta = (\beta', \beta'') \in \mathbb{F}_2^4 \times \mathbb{F}_2^{k-4}$, we have
$\sum_{y\in\mathbb{F}_2^k}(-1)^{h_0(y)+h_1(y+\beta)} = \sum_{y'\in\mathbb{F}_2^4}(-1)^{g_0(y')+g_1(y'+\beta')} \cdot \sum_{y''\in\mathbb{F}_2^{k-4}}(-1)^{w_0(y'')+w_1(y''+\beta'')}$. Then it follows from Item 6) of Lemma 3 and Item 1) of Lemma 4 that
$-3 \cdot 2^{k-2} - 3 \cdot 2^{(k+1)/2} \leq 2\sum_{y\in\mathbb{F}_2^k}(-1)^{h_0(y)+h_1(y+\beta)} \leq -2^{(k+5)/2}$.

4) For any $\beta = (\beta', \beta'') \in \mathbb{F}_2^4 \times \mathbb{F}_2^{k-4}$, by Lemma 5 we have $W_{h_0}(\beta) = W_{g_0}(\beta') \cdot W_{w_0}(\beta'')$. Thus, we have $|\max_{\beta \in \mathbb{F}_2^k} W_{h_0}(\beta)| = |\max_{\beta' \in \mathbb{F}_2^4} W_{g_0}(\beta')| \cdot |\max_{\beta'' \in \mathbb{F}_2^{k-4}} W_{w_0}(\beta'')| = 3 \cdot 2^{k-3} + 3 \cdot 2^{(k-1)/2}$ according to Item 3) of Lemma 3 and Item 3) of Lemma 4. Similarly, we can obtain that $|\max_{\beta \in \mathbb{F}_2^k} W_{h_1}(\beta)| = |\max_{\beta' \in \mathbb{F}_2^4} W_{g_1}(\beta')| \cdot |\max_{\beta'' \in \mathbb{F}_2^{k-4}} W_{w_1}(\beta'')| = 3 \cdot 2^{k-3} + 3 \cdot 2^{(k-1)/2}$.

5) Note that $W_{h_0}(\mathbf{0}) = W_{g_0}(\mathbf{0}') \cdot W_{w_0}(\mathbf{0}'') = 12 \cdot (2^{k-5} - 2^{(k-5)/2})$ and $W_{h_1}(\mathbf{0}) = W_{g_1}(\mathbf{0}') \cdot W_{w_1}(\mathbf{0}'') = -12 \cdot (2^{k-5} - 2^{(k-5)/2})$, where the values of $W_{g_0}(\mathbf{0}'), W_{g_1}(\mathbf{0}')$ from the two truth tables in Lemma 3 and the values of $W_{w_0}(\mathbf{0}''), W_{w_1}(\mathbf{0}'')$ can be found in the proof process of Item 3) of Lemma 4. Then we have $\mathrm{wt}(h_0) + \mathrm{wt}(h_1) = 2^k$. □

IV. Balanced Boolean functions with very low absolute indicator, strictly almost optimal nonlinearity and maximal algebraic degree

In this section, we present our main results of this paper. As we have mentioned in the introduction, bent functions possess the highest nonlinearity and has the lowest absolute indicator 0. Thus, a nature way to get balanced $2k$-variable Boolean function with high nonlinearity and low absolute indicator is to replace the all-zero values on a k-dimensional affine subspace of $\mathbb{F}_2^{2k}$ of a normal bent function with weight $2^{2k-1} - 2^{k-1}$ by a balanced Boolean function h in k variables. It was shown in [13, Lemma 20] that such function has absolute indicator no less than $2^k + \Delta_h$. Therefore, we need to at least replace the values on two k-dimensional affine subspace of $\mathbb{F}_2^{2k}$ by two functions in k variables.

Let us first introduce the partial spread ($\mathcal{PS}$) bent function and then propose a construction of balanced Boolean functions based on revising the simplest $\mathcal{PS}$ bent functions. We also mathematically proved that the constructed balanced Boolean functions have very low absolute indicator, strictly almost optimal nonlinearity and maximal algebraic degree.

The class of n-variable bent functions called $\mathcal{PS}$ was introduced by Dillon [4] in his PhD thesis. Any bent function in n variables belonging to this class is the union of $2^{\frac{n}{2}-1}$ or $2^{\frac{n}{2}-1}+1$ disjoint $\frac{n}{2}$-dimensional vector spaces of $\mathbb{F}_2^n$, where n is an even positive integer and "disjoint" means that any two of these subspaces intersect in $\mathbf{0}$ only. It should be note that any bent function in n variables belonging to this class has maximum algebraic degree $\frac{n}{2}$. Particularly, Dillon exhibited a subclass of $\mathcal{PS}$ in an explicit form, called $\mathcal{PS}_{ap}$ bent functions. It is well-known that for an arbitrary $n = 2k$ the finite field $\mathbb{F}_{2^n}$ can be viewed as a 2-dimensional vector space $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ over $\mathbb{F}_{2^k}$, which is equal to the disjoint union of its $2^k + 1$ lines through the origin. By arbitrarily picking up 2^{k-1} lines except for the origin as the support, Dillon presented a $\mathcal{PS}_{ap}$ bent function $r(x, y)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ as

$$r(x, y) = g\left(\frac{x}{y}\right)$$

where g is a balanced Boolean function on $\mathbb{F}_{2^k}$ with $g(0) = 0$, and $\frac{x}{y}$ is defined to be 0 if $y = 0$ (we shall always assume this kind of convention in the sequel).

In the rest of this section, our aim is to construct a class of balanced Boolean functions with very low absolute indicator, strictly almost optimal nonlinearity and maximal algebraic degree, via revising the simplest $\mathcal{PS}_{ap}$ bent function in $2k$ variables which is defined as

$$s(x, y) = \mathrm{Tr}_1^k\left(\frac{\lambda x}{y}\right), \tag{1}$$

where $(x, y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ and $\lambda \in \mathbb{F}_{2^k}^*$.

We now present the main construction.

Construction 1. *Let $n = 2k$ and $\lambda, \mu \in \mathbb{F}_{2^k}^*$, where $k \geq 9$ is an odd integer. We construct an n-variable Boolean function over $\mathbb{F}_{2^n}$ as follows*

$$f(x, y) = \begin{cases} h_0(y), & \text{if } x = 0 \\ h_1(y), & \text{if } x = \mu \\ s(x, y), & \text{if } x \neq 0 \text{ and } x \neq \mu \end{cases} \tag{2}$$

where $s(x, y)$ is the function over $\mathbb{F}_2^n$ defined by (1)*, and h_0, h_1 are the functions over $\mathbb{F}_2^k$ defined by Definition 3.*

It should be noted that in Construction 1 both functions h_0 and h_1 are defined over the vector space $\mathbb{F}_2^k$ and $s(x,y)$ are defined over the finite field $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$. As we mentioned in Section II, the vector space $\mathbb{F}_2^k$ is isomorphic to the finite field $\mathbb{F}_{2^k}$ through the choice of some basis of $\mathbb{F}_{2^k}$ over $\mathbb{F}_2$. Thus, the truth table of f can be given by identifying every element of the finite field $\mathbb{F}_{2^k}$ to an element of the vector space $\mathbb{F}_2^k$, see for instance Example 1. Indeed, the lower bounds on absolute indicator and nonlinearity of f given in the rest of this section do not depend on the choice of the basis of $\mathbb{F}_{2^k}$ over $\mathbb{F}_2$, and we shall interchange the elements belonging to $\mathbb{F}_2^k$ and $\mathbb{F}_{2^k}$ below.

Clearly, every Boolean function generated by Construction 1 is balanced according to Item 5) of Lemma 6 and the Boolean function $\mathrm{Tr}_1^k(\frac{\lambda x}{y})$ on variable $y \in \mathbb{F}_{2^k}$ is balanced over $\mathbb{F}_{2^k}$ for any fixed $\lambda x \neq 0$. In what follows, we give an upper bound on the absolute indicator, a lower bound on the nonlinearity, and the algebraic degree of the balanced Boolean functions generated by Construction 1, respectively.

A. The absolute indicator

In this subsection, we will obtain an upper bound on the absolute indicator of the functions generated by Construction 1. In order to do this, we need to give the following two results which are particularly useful to derive our bound.

Lemma 7. *([2]) For any positive integer k, the third-order nonlinearity of the function $h(y) = \mathrm{Tr}_1^k(\lambda/y)$, where $\lambda \in \mathbb{F}_{2^k}^*$, defined over $\mathbb{F}_{2^k}$ is*

$$\mathrm{nl}_3(h) \geq 2^{k-1} - \frac{1}{2}\sqrt{(2^k-1)\sqrt{2^{3k/2+3} + 3 \cdot 2^{k+1} - 2^{k/2+3} + 16}}.$$

Lemma 8 ([25])**.** *For any integer $k \geq 3$, let $C_{\mu,\nu}(\tau) = \sum_{x\in\mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_1^k(\frac{\mu}{x}) + \mathrm{Tr}_1^k(\frac{\nu}{x+\tau})}$. Then for any $\mu, \nu, \tau \in \mathbb{F}_{2^n}^*$, the value of $C_{\mu,\nu}(\tau)$ belongs to $[-2^{k/2+1} - 3, 2^{k/2+1} + 1]$ and is divisible by 4.*

Based on the above results, we shall now deduce an upper bound on the absolute indicator of the functions defined by Construction 1.

Theorem 1. *Let $f(x,y)$ be the $n = 2k$-variable Boolean function generated by Construction 1. Then we have $\Delta_f < 2^k - 2^{(k+3)/2}$ for $k \geq 23$.*

Proof. For any $(\alpha, \beta) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$. It follows from the definition of autocorrelation function that

$$C_f(\alpha,\beta) = \sum_{x\in\mathbb{F}_{2^k}} \sum_{y\in\mathbb{F}_{2^k}} (-1)^{f(x,y)+f(x+\alpha,y+\beta)},$$

which can be classified into the following four cases:

[**Case 1**.] $\alpha = \beta = 0$. Obviously, in this case we have $C_f(\alpha,\beta) = 2^n$.

[**Case 2**.] $\alpha = 0, \beta \in \mathbb{F}_{2^n}^*$. In this case we can deduce that

$$\begin{aligned} C_f(\alpha,\beta) &= \sum_{x\in\mathbb{F}_{2^k}} \sum_{y\in\mathbb{F}_{2^k}} (-1)^{f(x,y)+f(x+\alpha,y+\beta)} \\ &= \sum_{x\in\mathbb{F}_{2^k}\setminus\{0,\mu\}} \sum_{y\in\mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_1^k(\frac{\lambda x}{y} + \frac{\lambda x}{y+\beta})} + C_{h_0(\beta)} + C_{h_1(\beta)} \\ &= T_0 + C_{h_0(\beta)} + C_{h_1(\beta)}, \end{aligned}$$

where

$$T_0 = \sum_{x\in\mathbb{F}_{2^k}\setminus\{0,\mu\}} \sum_{y\in\mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_1^k(\frac{\lambda x}{y} + \frac{\lambda x}{y+\beta})}.$$

[**Case 3**.] $\alpha = \mu, \beta \in \mathbb{F}_{2^n}$. In this case we can get that

$$\begin{aligned} C_f(\alpha,\beta) &= \sum_{x\in\mathbb{F}_{2^k}} \sum_{y\in\mathbb{F}_{2^k}} (-1)^{f(x,y)+f(x+\alpha,y+\beta)} \\ &= \sum_{x\in\mathbb{F}_{2^k}\setminus\{0,\mu\}} \sum_{y\in\mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_1^k(\frac{\lambda x}{y} + \frac{\lambda(x+\alpha)}{y+\beta})} + 2\sum_{y\in\mathbb{F}_{2^k}} (-1)^{h_0(y)+h_1(y+\beta)} \\ &= T_1 + 2\sum_{y\in\mathbb{F}_{2^k}} (-1)^{h_0(y)+h_1(y+\beta)}, \end{aligned}$$

where

$$T_1 = \sum_{x\in\mathbb{F}_{2^k}\setminus\{0,\mu\}} \sum_{y\in\mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_1^k(\frac{\lambda x}{y}+\frac{\lambda(x+\alpha)}{y+\beta})}.$$

[**Case 4**.] $\alpha \in \mathbb{F}_{2^n} \setminus \{0,\mu\}, \beta \in \mathbb{F}_{2^n}$.

$$\begin{aligned} C_f(\alpha,\beta) &= \sum_{x\in\mathbb{F}_{2^k}} \sum_{y\in\mathbb{F}_{2^k}} (-1)^{f(x,y)+f(x+\alpha,y+\beta)} \\ &= \sum_{x\in\mathbb{F}_{2^k}\setminus\{0,\mu,\alpha,\alpha+\mu\}} \sum_{y\in\mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_1^k(\frac{\lambda x}{y}+\frac{\lambda(x+\alpha)}{y+\beta})} \\ &\quad +2\sum_{y\in\mathbb{F}_{2^k}} (-1)^{h_0(y+\beta)+\mathrm{Tr}_1^k(\frac{\lambda\alpha}{y})} + 2\sum_{y\in\mathbb{F}_{2^k}} (-1)^{h_1(y+\beta)+\mathrm{Tr}_1^k(\frac{\lambda(\mu+\alpha)}{y})} \\ &= T_2 + 2\sum_{y\in\mathbb{F}_{2^k}} (-1)^{h_0(y+\beta)+\mathrm{Tr}_1^k(\frac{\lambda\alpha}{y})} + 2\sum_{y\in\mathbb{F}_{2^k}} (-1)^{h_1(y+\beta)+\mathrm{Tr}_1^k(\frac{\lambda(\mu+\alpha)}{y})}, \end{aligned}$$

where

$$T_2 = \sum_{x\in\mathbb{F}_{2^k}\setminus\{0,\mu,\alpha,\alpha+\mu\}} \sum_{y\in\mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_1^k(\frac{\lambda x}{y}+\frac{\lambda(x+\alpha)}{y+\beta})}.$$

We shall now evaluate the values of T_0, T_1 and T_2. Note that the function $s(x,y) = \mathrm{Tr}_1^k(\frac{\lambda x}{y}) \in \mathcal{B}_n$ defined by (1) is the simplest $\mathcal{PS}_{ap}$ bent function. Thus, we have $C_s(\alpha,\beta) = 0$ for any $(\alpha,\beta) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \setminus \{(0,0)\}$, according to Lemma 1. Similar to the Cases 2-4 above, by the definition of autocorrelation function of the bent function s we have

$$\begin{cases} T_0 + 2^k + \sum\limits_{y\in\mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_1^k(\frac{\lambda\mu}{y}+\frac{\lambda\mu}{y+\beta})} = 0, & \text{if } \alpha = 0, \beta \in \mathbb{F}_{2^n}^* \\ T_1 + 2\sum\limits_{y\in\mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_1^k(\frac{\lambda\mu}{y})+0} = 0, & \text{if } \alpha = \mu, \beta \in \mathbb{F}_{2^n} \\ T_2 + 2\sum\limits_{y\in\mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_1^k(\frac{\lambda\alpha}{y})+0} + 2\sum\limits_{y\in\mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_1^k(\frac{\lambda\mu}{y}+\frac{\lambda(\mu+\alpha)}{y+\beta})} = 0, & \text{if } \alpha \in \mathbb{F}_{2^n} \setminus \{0,\mu\}, \beta \in \mathbb{F}_{2^n} \end{cases}$$

Let $t = \max\{|t'| \ : \ t' \in [-2^{k/2+1}-3, 2^{k/2+1}+1] \text{ and } t' = 0 \pmod 4\}$. On the one hand, according to Lemma 8, we have $|\sum_{y\in\mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_1^k(\frac{\lambda\mu}{y}+\frac{\lambda(\mu+\alpha)}{y+\beta})}| \le t$ when $\lambda\mu \ne 0$, $\beta \in \mathbb{F}_{2^k}^*$ and $\alpha \in \mathbb{F}_{2^k}$. On the other hand, note that $\sum_{y\in\mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_1^k(\lambda\mu/y)} = 0$ if $\lambda\mu \ne 0$. Therefore, we immediately get $-2^k - t \le T_0 \le -2^k + t$, $T_1 = 0$ and $-2t \le T_2 \le 2t$. Hence, by Item 2) of Lemma 6 we easily have $-2^k - t + 2^{(k+5)/2} \le C_f(\alpha,\beta) \le 2^{k-1} + t$ if $\alpha = 0, \beta \in \mathbb{F}_{2^n}^*$; by Item 3) of Lemma 6 we directly have $-3\cdot 2^{k-2} - 3\cdot 2^{(k+1)/2} \le C_f(\alpha,\beta) \le -2^{(k+5)/2}$ if $\alpha = \mu, \beta \in \mathbb{F}_{2^n}$.

Note that Lemma 7 implies that the Hamming distance from $\mathrm{Tr}_1^k(\frac{\gamma}{y})$, where $\gamma \in \mathbb{F}_{2^k}^*$, to any function h of degree no more than 3 is greater than $2^{k-1} - \frac{1}{2}\sqrt{(2^k-1)\sqrt{2^{3k/2+3} + 3\cdot 2^{k+1} - 2^{k/2+3} + 16}}$, which is equivalent to saying that $|\sum_{y\in\mathbb{F}_{2^k}} (-1)^{h(y)+\mathrm{Tr}_1^k(\frac{\gamma}{y})}| \le 2^k - 2\mathrm{nl}_3(h)$. Further, both $h_0(y+\beta)$ and $h_1(y+\beta)$ have algebraic degree 3 since both $h_0(y)$ and $h_1(y)$ have algebraic degree 3 by Item 1) of Lemma 6. Thus, we have $|\sum_{y\in\mathbb{F}_{2^k}} (-1)^{h_0(y+\beta)+\mathrm{Tr}_1^k(\frac{\lambda\alpha}{y})}| \le 2^k - 2\mathrm{nl}_3(h) \le l$ and $|\sum_{y\in\mathbb{F}_{2^k}} (-1)^{h_1(y+\beta)+\mathrm{Tr}_1^k(\frac{\lambda(\mu+\alpha)}{y})}| \le 2^k - 2\mathrm{nl}_3(h) \le l$, where $l = \sqrt{(2^k-1)\sqrt{2^{3k/2+3} + 3\cdot 2^{k+1} - 2^{k/2+3} + 16}}$. Recall that $-2t \le T_2 \le 2t$.

Therefore, we have $|C_f(\alpha,\beta)| \le 4l + 2t$ if $\alpha \in \mathbb{F}_{2^n} \setminus \{0,\mu\}, \beta \in \mathbb{F}_{2^n}$. Note that $t < 2^{\frac{k+3}{2}}$ and $l < \sqrt{(2^k-1)(2^{(3k+6)/4} + 2^{(k+1)/4})} < 2^{k/2}(2^{(3k+6)/8} + 2^{-(k+12)/8}) = 2^{(7k+6)/8} + 2^{(3k-12)/8}$ for odd $k \ge 3$. Form what has been discussed above, we conclude that

$$|C_f(\alpha,\beta)| < \begin{cases} 2^k - 2^{\frac{k+3}{2}}, & \text{if } \alpha = 0, \beta \in \mathbb{F}_{2^n}^* \\ 2^{k-1} + 2^{k-2} + 2^{\frac{k+3}{2}} + 2^{\frac{k+1}{2}}, & \text{if } \alpha = \mu, \beta \in \mathbb{F}_{2^n} \\ 2^{\frac{7k+22}{8}} + 2^{\frac{3k+4}{8}} + 2^{\frac{k+5}{2}}, & \text{if } \alpha \in \mathbb{F}_{2^n} \setminus \{0,\mu\}, \beta \in \mathbb{F}_{2^n} \end{cases}$$

So we have

$$\Delta_f < \max\{2^k - 2^{\frac{k+3}{2}}, 2^{k-1} + 2^{k-2} + 2^{\frac{k+3}{2}} + 2^{\frac{k+1}{2}}, 2^{\frac{7k+22}{8}} + 2^{\frac{3k+4}{8}} + 2^{\frac{k+5}{2}}\}.$$

Note that $(2^k - 2^{\frac{k+3}{2}}) - (2^{k-1} + 2^{k-2} + 2^{\frac{k+3}{2}} + 2^{\frac{k+1}{2}}) = 2^{k-2} - 5 \cdot 2^{\frac{k+1}{2}} > 2^{k-2} - 2^{\frac{k+7}{2}} \geq 0$ for $k \geq 11$. Note also that $(2^k - 2^{\frac{k+3}{2}}) - (2^{\frac{7k+22}{8}} + 2^{\frac{3k+4}{8}} + 2^{\frac{k+5}{2}}) = 2^{\frac{7k+22}{8}}(2^{\frac{k-22}{8}} - 1) - 2^{\frac{3k+4}{8}} - 3 \cdot 2^{\frac{k+3}{2}} > 2^{\frac{7k+22}{8}} - 2^{\frac{3k+4}{8}} - 3 \cdot 2^{\frac{k+3}{2}} > 2^{\frac{7k+22}{8}} - 2^{\frac{3k+4}{8}} - 2^{\frac{k+7}{2}} > 2^{\frac{7k+22}{8}} - 2^{\frac{4k+28}{8}} - 2^{\frac{k+7}{2}} = 2^{\frac{7k+22}{8}} - 2^{\frac{4k+36}{8}} \geq 0$ for $k \geq 23$. Thus we have $\Delta_f < 2^k - 2^{\frac{k+3}{2}}$ for $k \geq 23$. This completes the proof. □

Thus, we present a construction and prove for the first time that it is possible to obtain an infinite class of balanced functions f on n variables with $\Delta_f < 2^{\frac{n}{2}}$, when $n \equiv 2 \pmod 4$ and $n \geq 46$. The constraint $n \equiv 2 \pmod 4$ comes as $n = 2k$, where k is odd, and the bound $n \geq 46$ comes from algebraic manipulation to show that Δ_f is indeed less than $2^{\frac{n}{2}}$. However, the proof is one directional. Thus, in case we can actually construct the function on lower number of variables, that might have $\Delta_f < 2^{\frac{n}{2}}$ too. The main trick here comes from Lemma 6, where we construct functions h_0, h_1 on k variables, $k \geq 9$, odd. Thus our construction can be experimentally checked for the minimum value of $n = 2k = 18$. This we present in the following example and show that our construction indeed achieves $\Delta_f = 480 < 2^{\frac{18}{2}}$, though it is not explicitly proved in Theorem 1. One may access the Boolean function and the related programs at [24].

Example 1. *Let $n = 2k$ where $k = 9$. Let ω be a root of the primitive polynomial $x^9 + x^4 + 1$ and $1, \omega, \omega^2, \cdots, \omega^8$ be a basis of $\mathbb{F}_{2^9}$. Then every element $x \in \mathbb{F}_{2^9}$ can be uniquely expressed as $x = x_1 + x_2\omega + x_3\omega^2 + \cdots + x_9\omega^8$ and hence $x \in \mathbb{F}_{2^9}$ is identified with a vector $(x_1, x_2, x_3, \cdots, x_8, x_9) \in \mathbb{F}_2^9$. By a Matlab program, we have $\mathrm{Tr}_1^k(w) = \mathrm{Tr}_1^k(w^2) = \mathrm{Tr}_1^k(w^3) = \mathrm{Tr}_1^k(w^4) = \mathrm{Tr}_1^k(w^6) = \mathrm{Tr}_1^k(w^7) = \mathrm{Tr}_1^k(w^8) = 0$ and $\mathrm{Tr}_1^k(1) = \mathrm{Tr}_1^k(w^5) = 1$. In this example we take $\lambda = \mu = 1 \in \mathbb{F}_{2^9}$, $s_0 = [0,0,0,0,0,0,1,1,0,1,0,1,0,1,1,0]$ and $s_1 = [0,0,0,0,0,1,0,1,0,1,1,0,0,0,1,1]$. Then we can obtain the truth table of f by computer program. For example, consider that we want to get the value of f at point $(0,0,0,0,0,1,0,0,1,0,0,0,0,0,0,0,1,1) \in \mathbb{F}_2^{18}$. We have $(0,0,0,0,0,1,0,0,1)$ is identified with $w^5 + w^8 = w^{425}$ and $(0,0,0,0,0,0,0,1,1)$ is identified with $w^7 + w^8 = w^{137}$. Hence, $f(0,0,0,0,0,1,0,0,1,0,0,0,0,0,0,0,1,1) = \mathrm{Tr}_1^k(\frac{w^{425}}{w^{137}}) = \mathrm{Tr}_1^k(w^{288}) = \mathrm{Tr}_1^k(1 + w^2 + w^3 + w^7 + w^8) = \mathrm{Tr}_1^k(1) + \mathrm{Tr}_1^k(w^2) + \mathrm{Tr}_1^k(w^3) + \mathrm{Tr}_1^k(w^7) + \mathrm{Tr}_1^k(w^8) = 1$. After constructing the truth table of this function, we checked by computer program that f has absolute indicator $480 < 2^9 = 512$. Further, one can also check that the function has nonlinearity $130664 > 2^{17} - 2^9 = 130560$ and algebraic degree 17.*

We found similar results for $n = 22$ and 26 too (please refer to Table Comparisonlb). However, due to high computational complexity, we could not check the cases $n = 30, 34$ and 38. From $n = 46$ and higher values with $n \equiv 2 \bmod 4$, the results are proved theoretically.

B. Nonlinearity

We shall now obtain a lower bound on the nonlinearity of the Boolean functions generated by Construction 1. This requires the following two results.

Lemma 9 ([11]). *For any positive integer k and arbitrary $a \in \mathbb{F}_{2^k}^*$, the Walsh spectrum of $\mathrm{Tr}_1^k(\frac{a}{x})$ defined on $\mathbb{F}_{2^k}$ can take any value divisible by 4 in the range $[-2^{k/2+1} + 1, 2^{k/2+1} + 1]$.*

Lemma 10. *Let k be a positive integer and λ be a nonzero element of $\mathbb{F}_{2^k}$. For any $(\alpha, \beta) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$, we define $U_{(\alpha,\beta)} = \sum_{x \in \mathbb{F}_{2^k}^*} \sum_{y \in \mathbb{F}_{2^k}} (-1)^{\mathrm{Tr}_1^k(\frac{\lambda x}{y} + \alpha x + \beta y)}$. Then we have*

$$U_{(\alpha,\beta)} = \begin{cases} 0, & \text{if } \beta = 0 \\ 2^k(-1)^{\mathrm{Tr}_1^k(\frac{\beta\lambda}{\alpha})}, & \text{if } \beta \neq 0 \end{cases}$$

Proof. Basically, our discuss is built on the fact that $\sum_{x\in\mathbb{F}_{2^k}^*}(-1)^{\mathrm{Tr}_1^k(\gamma x)} = 2^k-1$ if $\gamma = 0$ and $\sum_{x\in\mathbb{F}_{2^k}^*}(-1)^{\mathrm{Tr}_1^k(\gamma x)} = -1$ otherwise. We have

$$\begin{aligned} U_{(\alpha,\beta)} &= \sum_{x\in\mathbb{F}_{2^k}^*}\sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^k(\frac{\lambda x}{y}+\alpha x+\beta y)} \\ &= \sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^k(\beta y)}\sum_{x\in\mathbb{F}_{2^k}^*}(-1)^{\mathrm{Tr}_1^k((\frac{\lambda}{y}+\alpha)x)} \\ &= (2^k-1)(-1)^{\mathrm{Tr}_1^k(\frac{\beta\lambda}{\alpha})} - \sum_{y\in\mathbb{F}_{2^k}\setminus\{\frac{\beta\lambda}{\alpha}\}}(-1)^{\mathrm{Tr}_1^k(\beta y)} \\ &= 2^k(-1)^{\mathrm{Tr}_1^k(\frac{\beta\lambda}{\alpha})} - \sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^k(\beta y)} \\ &= \begin{cases} 0, & \text{if } \beta = 0 \\ 2^k(-1)^{\mathrm{Tr}_1^k(\frac{\beta\lambda}{\alpha})}, & \text{if } \beta \neq 0 \end{cases} \end{aligned}$$

This completes the proof. □

Theorem 2. *Let $f(x,y)$ be the $n = 2k$-variable Boolean function generated by Construction 1. Then we have $\mathrm{nl}(f) > 2^{n-1} - 7\cdot 2^{k-3} - 5\cdot 2^{\frac{k-1}{2}}$, which is strictly almost optimal nonlinearity for integer $k \geq 11$.*

Proof. For any $(\alpha,\beta)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}$,the Walsh transform of f at (α,β) can be written as

$$\begin{aligned} & W_f(\alpha,\beta) \\ = {} & \sum_{x\in\mathbb{F}_{2^k}}\sum_{y\in\mathbb{F}_{2^k}}(-1)^{f(x,y)+\mathrm{Tr}_1^k(\alpha x)+\mathrm{Tr}_1^k(\beta y)} \\ = {} & \sum_{x\in\mathbb{F}_{2^k}\setminus\{0,\mu\}}(-1)^{\mathrm{Tr}_1^k(\alpha x)}\sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^k(\frac{\lambda x}{y}+\beta y)} + (-1)^{\mathrm{Tr}_1^k(\alpha\mu)}W_{h_1}(\beta) + W_{h_0}(\beta) \\ = {} & \sum_{x\in\mathbb{F}_{2^k}^*}\sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^k(\frac{\lambda x}{y}+\alpha x+\beta y)} + (-1)^{\mathrm{Tr}_1^k(\alpha\mu)}W_{h_1}(\beta) + W_{h_0}(\beta) - \sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^k(\frac{\lambda\mu}{y}+\alpha\mu+\beta y)} \\ = {} & U_{(\alpha,\beta)} + (-1)^{\mathrm{Tr}_1^k(\alpha\mu)}W_{h_1}(\beta) + W_{h_0}(\beta) - \sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^k(\frac{\lambda\mu}{y}+\alpha\mu+\beta y)}. \end{aligned}$$

So we have

$$\begin{aligned} |W_f(\alpha,\beta)| &= |U_{(\alpha,\beta)} + (-1)^{\mathrm{Tr}_1^k(\alpha\mu)}W_{h_1}(\beta) + W_{h_0}(\beta) - \sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^k(\frac{\lambda\mu}{y}+\alpha\mu+\beta y)}| \\ &\leq |U_{(\alpha,\beta)}| + |W_{h_1}(\beta)| + |W_{h_0}(\beta)| + |\sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^k(\frac{\lambda\mu}{y}+\alpha\mu+\beta y)}| \\ &= \begin{cases} |W_{h_1}(\beta)| + |W_{h_0}(\beta)| + |\sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^k(\frac{\lambda\mu}{y}+\alpha\mu+\beta y)}|, & \text{if } \beta = 0 \\ 2^k + |W_{h_1}(\beta)| + |W_{h_0}(\beta)| + |\sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^k(\frac{\lambda\mu}{y}+\alpha\mu+\beta y)}|, & \text{if } \beta \neq 0 \end{cases}, \end{aligned}$$

where Lemma 10 is used in the last identity. Then, by Lemmas 6 and 9, we immediately get that

$$\begin{aligned} |\max_{(\alpha,\beta)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}} W_f(\alpha,\beta)| &\leq 2^k + 2\cdot(3\cdot 2^{k-3} + 3\cdot 2^{\frac{k-1}{2}}) + 2^{\frac{k+3}{2}} \\ &= 2^k + 3\cdot 2^{k-2} + 10\cdot 2^{\frac{k-1}{2}}. \end{aligned}$$

Therefore, we have $\mathrm{nl}(f) > 2^{n-1} - 7\cdot 2^{k-3} - 5\cdot 2^{\frac{k-1}{2}}$. □

C. Algebraic degree

It is well-known that the maximum algebraic degree of a balanced Boolean functions in n variables is $n-1$. We shall now discuss the algebraic degrees of the functions given by Construction 1.

Theorem 3. *The $n = 2k$-variable Boolean function $f(x, y)$ defined by Construction 1 has maximum algebraic degree $n - 1$.*

Proof. Clearly, f has algebraic degree at most $n-1$ since its Hamming weight is even. Note that f can be written as $f(x, y) = s(x, y) + f'(x, y)$, where $s \in \mathcal{B}_n$ is defined by (1) and $f' \in \mathcal{B}_n$ is defined as follows

$$f'(x,y) = \begin{cases} h_1(y) + \mathrm{Tr}_1^k(\frac{\lambda\mu}{y}), & \text{if } x = \mu \\ h_0(y), & \text{if } x = 0 \\ 0, & \text{otherwise} \end{cases}$$

Note that s is a $\mathcal{PS}_{ap}$ bent function and so has algebraic degree k. Thus, for proving that f has algebraic degree $n-1$, we only need to prove that f' has algebraic degree no less than $n-1$. Let us denote by $h_1'(y)$ the function $h_1(y) + \mathrm{Tr}_1^k(\frac{\lambda\mu}{y})$. By Lagrange interpolation we have $f'(x,y) = \sum_{(a,b)\in\mathrm{supp}(f')} \big(1 + (x+a)^{2^k-1}\big)\big(1 + (y + b)^{2^k-1}\big) = \sum_{(0,b)\in\mathrm{supp}(f')} \big(1 + x^{2^k-1}\big)\big(1 + (y+b)^{2^k-1}\big) + \sum_{(\mu,b)\in\mathrm{supp}(f')} \big(1 + (x+\mu)^{2^k-1}\big)\big(1 + (y+b)^{2^k-1}\big) = \big(1+x^{2^k-1}\big) \sum_{b\in\mathrm{supp}(h_0)} \big(1+(y+b)^{2^k-1}\big) + \big(1+(x+\mu)^{2^k-1}\big) \sum_{b\in\mathrm{supp}(h_1')} \big(1+(y+b)^{2^k-1}\big) = \big(1+x^{2^k-1}\big)h_0 + \big(1+(x+\mu)^{2^k-1}\big)h_1'$. Note that the algebraic degree of $\mathrm{Tr}_1^k(\frac{\lambda\mu}{y})$ defined on $\mathbb{F}_{2^k}$ equals $k-1$ since $\mathrm{Tr}_1^k(\frac{\lambda\mu}{y}) = \mathrm{Tr}_1^k(\lambda\mu y^{2^k-2})$ and the Hamming weight of the binary expansion of $2^k - 2$ is $k-1$. Note also that both h_0 and h_1 have algebraic degree 3 according to Item 1) of Lemma 6. Thus, we can easily see that the term $x^{2^k-1}(\lambda\mu y^{2^k-2}) = \lambda\mu x^{2^k-1}y^{2^k-2}$ is included in $\big(1 + (x+\mu)^{2^k-1}\big)h_1'$ and this term will never be canceled by other terms of f'. Hence, the algebraic degree of f' is no less than $k + (k-1) = n-1$. This implies that f has algebraic degree $n-1$. This completes the proof. □

V. Conclusion

Since the conjecture had been proposed almost two decades back, that $\Delta_f \geq 2^{\frac{n}{2}}$ [27], examples of balanced Boolean functions in even variables n with absolute indicator strictly less than $2^{\frac{n}{2}}$ could only be achieved for $n = 10, 14$ by computer search techniques. In this paper, we could mathematically construct an infinite class of balanced Boolean function on n variables ($n \equiv 2 \bmod 4$) with absolute indicator strictly less than $2^{\frac{n}{2}} - 2^{\frac{n+6}{4}}$, nonlinearity strictly greater than $2^{n-1} - 7 \cdot 2^{\frac{n}{2}-3} - 5 \cdot 2^{\frac{n-2}{4}}$ and algebraic degree $n-1$, where $n \geq 46$. This is the first time that an infinite class of balanced Boolean functions with absolute indicator strictly less than $2^{\frac{n}{2}}$ could be obtained. While we could theoretically prove the result for $n \geq 46$, our construction also works for lesser number of variables. In fact, our construction starts from $n = 18$ and for $n = 18, 22$, and 26, we could check that the constructed balanced functions f achieve $\Delta_f < 2^{\frac{n}{2}}$ with nonlinearity $> 2^{n-1} - 2^{\frac{n}{2}}$ and algebraic degree $n-1$. Given our result, we have now two different classes left to achieve similar results.

- Functions on n variables, where $n \equiv 0 \bmod 4$: In this case, we do not have any example yet to disprove the conjecture of [27]. Thus the immediate question here is to at least find an example (better if a theoretical construction is obtained) or to show that it is not at all possible to construct such functions.
- Functions on n variables, where n is odd: In this case, we have examples where the conjecture is disproved, namely for $n = 9, 11$ in [7], $n = 15$ in [15] and $n = 21$ in [14], [10]. Thus a general construction in this case would be of interest.

We leave these questions for future research.

References

[1] Linda Burnett, William Millan, Edward Dawson, and Andrew Clark. Simpler methods for generating better Boolean functions with good cryptographic properties. *Australasian Journal of Combinatorics*, 29:231–248, 2004.

[2] Claude Carlet. Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications. *IEEE Transactions on Information Theory*, 54(3):1262–1272, 2008.

[3] John A Clark, Jeremy L Jacob, Susan Stepney, Subhamoy Maitra, and William Millan. Evolving Boolean functions satisfying multiple criteria. In *Progress in Cryptology–INDOCRYPT 2002*, pages 246–259. Springer, 2002.

[4] John F Dillon. *Elementary Hadamard difference sets*. PhD thesis, Univ. of Maryland, 1974.

[5] Cunsheng Ding, Guozhen Xiao, and Weijuan Shan. *The stability theory of stream ciphers*, volume 561. Springer, 1991.

[6] Hans Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. In *Fast Software Encryption*, pages 61–74. Springer, 1995.

[7] Selçuk Kavut, Subhamoy Maitra, and Melek D Yücel. Search for Boolean functions with excellent profiles in the rotation symmetric class. *IEEE Transactions on Information Theory*, 53(5):1743–1751, 2007.

[8] Selçuk Kavut and Melek D Yücel. Improved cost function in the design of Boolean functions satisfying multiple criteria. In *Progress in Cryptology-INDOCRYPT 2003*, pages 121–134. Springer, 2003.

[9] Selçuk Kavut and Melek D Yücel. A new algorithm for the design of strong Boolean functions. In *First National Cryptology Symposium*, pages 95–105, 2005.

[10] Selçuk Kavut. Correction to the paper: Patterson-Wiedemann construction revisited. *Discrete Applied Mathematics*, 202: 185–187 (2016)

[11] Gilles Lachaud and Jacques Wolfmann. The weights of the orthogonals of the extended quadratic binary goppa codes. *IEEE Transactions on Information Theory*, 36(3):686–692, 1990.

[12] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error-correcting codes*, volume 16. Elsevier, 1977.

[13] Subhamoy Maitra. Highly nonlinear balanced Boolean functions with very good autocorrelation property. *Electronic Notes in Discrete Mathematics*, 6:481–490, 2001.

[14] Sugata Gangopadhyay, Pradeep H. Keskar and Subhamoy Maitra. Patterson-Wiedemann Construction Revisited. In *Discrete Mathematics*, Volume 306, Issue 14, Pages 1540–1556, 2006. A special issue containing selected papers from "R.C. Bose Centennial Symposium on discrete mathematics and Applications" December 2002.

[15] Subhamoy Maitra and Palash Sarkar. Modifications of patterson-wiedemann functions for cryptographic applications. *IEEE Transactions on Information Theory*, 48(1):278–284, 2002.

[16] James Massey. Shift-register synthesis and BCH decoding. *IEEE Transactions on Information Theory*, 15(1):122–127, 1969.

[17] Willi Meier and Othmar Staffelbach. Fast correlation attacks on stream ciphers. In *Advances in Cryptology–EUROCRYPT 1988*, pages 301–314. Springer, 1988.

[18] Sondre Ronjom and Tor Helleseth. A new attack on the filter generator. *IEEE Transactions on Information Theory*, 53(5):1752–1758, 2007.

[19] Oscar S Rothaus. On "bent" functions. *Journal of Combinatorial Theory, Series A*, 20(3):300–305, 1976.

[20] Rainer A Rueppel and Othmar Staffelbach. Products of linear recurring sequences with maximum complexity. *IEEE Transactions on Information Theory*, 33(1):124–131, 1987.

[21] Palash Sarkar and Subhamoy Maitra. Cross-correlation analysis of cryptographically useful boolean functions and s-boxes. *Theory Comput. Syst.*, 35(1):39–57, 2002.

[22] Jennifer Seberry, Xian-Mo Zhang, and Yuliang Zheng. *On Constructions and Nonlinearity of Correlation Immune Functions*, pages 181–199. Springer Berlin Heidelberg, Berlin, Heidelberg, 1994.

[23] Claude E Shannon. Communication theory of secrecy systems. *Bell system technical journal*, 28(4):656–715, 1949.

[24] Deng Tang and Subhamoy Maitra. Data and C Codes for balanced Boolean functions with $\Delta_f < 2^{\frac{n}{2}}$ for n even. Available at http://www.isical.ac.in/~subho/delta/ac1.html, November 2016.

[25] Deng Tang, Claude Carlet, and Xiaohu Tang. Differentially 4-uniform bijections by permuting the inverse function. *Designs, Codes and Cryptography*, pages 1–25, 2013.

[26] A F Webster and Stafford E Tavares. On the design of S-boxes. In *Advances in Cryptology–CRYPTO 1985 Proceedings*, pages 523–534. Springer, 1986.

[27] Xian-Mo Zhang and Yuliang Zheng. GAC – the criterion for global avalanche characteristics of cryptographic functions. In *Journal of Universal Computer Science*, pages 320–337. Springer, 1996.