

Research Article

On Negabent Functions and Nega-Hadamard Transform

Zepeng Zhuo and Jinfeng Chong

School of Mathematical Science, Huaibei Normal University, Huaibei, Anhui 235000, China

Correspondence should be addressed to Zepeng Zhuo; zzp781021@sohu.com

Received 29 June 2015; Revised 23 October 2015; Accepted 26 October 2015

Academic Editor: Laura Gardini

Copyright © 2015 Z. Zhuo and J. Chong. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The Boolean function which has equal absolute spectral values under the nega-Hadamard transform is called negabent function. In this paper, the special Boolean functions by concatenation are presented. We investigate their nega-Hadamard transforms, nega-autocorrelation coefficients, sum-of-squares indicators, and so on. We establish a new equivalent statement on $f_1 \parallel f_2$ which is negabent function. Based on them, the construction for generating the negabent functions by concatenation is given. Finally, the function expressed as $f(Ax \oplus a) \oplus b \cdot x \oplus c$ is discussed. The nega-Hadamard transform and nega-autocorrelation coefficient of this function are derived. By applying these results, some properties are obtained.

1. Introduction

Rothaus [1] introduced the class of bent functions which play an important role in cryptography and error correcting coding (where they are used to define optimum codes such as the Kerdock codes). The bent functions are those Boolean functions whose Hamming distance to the set of all affine functions is maximum. Equivalently, their spectrum with respect to the Walsh-Hadamard transform is flat (i.e., all spectral values have the same absolute value). The Walsh-Hadamard transform is an example of a unitary transformation on the space of all Boolean functions. Riera and Parker [2] considered some generalized bent criteria for Boolean functions by analyzing Boolean functions that have a flat spectrum with respect to one or more transforms chosen from a set of unitary transforms. The transforms chosen by Riera and Parker are n -fold tensor products of the identity mapping $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, Walsh-Hadamard transformation $(1/\sqrt{2}) \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and nega-Hadamard transformation $(1/\sqrt{2}) \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$, where $i^2 = -1$. Riera and Parker [2] mentioned that this choice is motivated by local unitary transforms that play an important role in the structural analysis of pure n -qubit stabilizer quantum states. As in the case of the Walsh-Hadamard transform, a Boolean function whose nega-Hadamard magnitude spectrum is flat is said to be

negabent. Moreover, a Boolean function is called bent-negabent if it is both bent and negabent. For instance, the 6-variable function $f(x) = (x_1 \oplus x_2 \oplus x_1 x_2 \oplus x_2 x_3) x_4 \oplus (x_3 \oplus x_1 x_2 \oplus x_2 x_3) x_5 \oplus (x_1 \oplus x_3) x_6$ is a cubic negabent function and the 4-variable function $g(y) = y_1 y_2 \oplus y_2 y_3 \oplus y_3 y_4$ is bent-negabent.

Negabent functions and bent-negabent functions have been extensively studied during the last few years [3–11]. Parker and Pott [3] presented several constructions and classifications on bent-negabent. Schmidt et al. [4] constructed a subclass of the Maiorana-McFarland class of bent functions in which all functions are also negabent. Also, they provided an upper bound on the algebraic degree of any bent-negabent Boolean function from the Maiorana-McFarland class. Sarkar [5] studied the symmetric negabent functions and obtained that a symmetric function is negabent if and only if it is affine. Stănică et al. [6, 9] gave the detailed study of some of properties of nega-Hadamard transform and derived several results on negabentness of concatenations. They pointed out that the algebraic degree of an n -variable negabent function is at most $\lceil n/2 \rceil$. In [7], Gangopadhyay and Chaturvedi developed the technique of constructing bent-negabent functions by using complete mapping polynomials. Sarkar [8] considered negabent functions that have trace representation and completely characterized negabent quadratic

monomial functions. The necessary and sufficient condition for a Maiorana-McFarland bent function to be a negabent function was presented in [8]. Su et al. [10] gave necessary and sufficient conditions for Boolean functions to be a negabent function for both an even and an odd number of variables and also determined the nega-Hadamard transform distribution of negabent functions. Further, a method to construct bent-negabent functions was provided. In [11], Zhang et al. presented two methods for constructing bent-negabent functions by using the indirect sum construction (proposed by Carlet in 2004 [12]).

2. Definitions and Notations

In this section we introduce a few basic concepts and notations. Let F_2 denote the finite field with two elements. We denote by \mathcal{B}_n the set of all Boolean functions of n -variable, that is, of all the functions from F_2^n into F_2 . The set of integers, real numbers, and complex numbers are denoted by \mathbf{Z} , \mathbf{R} , and \mathbf{C} , respectively. The addition over \mathbf{Z} , \mathbf{R} , and \mathbf{C} is denoted by $+$, \sum_i . The addition over F_2^n for all $n \geq 1$ is denoted by \oplus , \bigoplus_i . The Hamming weight $wt(x)$ of an element $x = (x_1, x_2, \dots, x_n) \in F_2^n$ is the number of ones in x ; that is, $wt(x) = \sum_{i=1}^n x_i$. We say that a Boolean function is balanced if its truth table contains an equal number of 0's and 1's; that is, if its Hamming weight equals $wt(f) = 2^{n-1}$. The Hamming distance between two functions $f(x)$ and $g(x)$, denoted by $d(f, g)$, is the Hamming weight of $f \oplus g$; that is, $d(f, g) = wt(f \oplus g)$.

Any Boolean function $f(x) \in \mathcal{B}_n$, where $x = (x_1, x_2, \dots, x_n) \in F_2^n$, is generally represented by its algebraic normal form (ANF):

$$f(x_1, x_2, \dots, x_n) = \bigoplus_{u \in F_2^n} \lambda_u \left(\prod_{i=1}^n x_i^{u_i} \right), \quad (1)$$

where $\lambda_u \in F_2$ and $u = (u_1, u_2, \dots, u_n) \in F_2^n$. The algebraic degree of $f(x)$, denoted by $\deg(f)$, is the maximal value of $wt(u)$ such that $\lambda_u \neq 0$. A Boolean function is affine if there exists no term of degree strictly greater than 1 in the ANF and the set of all affine functions is denoted by A_n . An affine function with constant term equal to zero is called a linear function. Any linear function on F_2^n is denoted by $x \cdot \omega = x_1\omega_1 \oplus x_2\omega_2 \oplus \dots \oplus x_n\omega_n$, where $x, \omega \in F_2^n$. The nonlinearity of an n -variable function $f(x)$ is $nl(f) = \min_{g \in A_n} (d(f, g))$, that is, the distance from the set of all n -variable affine functions. If $x = (x_1, x_2, \dots, x_n) \in F_2^n$ and $y = (y_1, y_2, \dots, y_n) \in F_2^n$, we define the scalar (or inner) product, respectively, as the intersection by

$$\begin{aligned} x \cdot y &= x_1y_1 \oplus x_2y_2 \oplus \dots \oplus x_ny_n, \\ x * y &= (x_1y_1, x_2y_2, \dots, x_ny_n). \end{aligned} \quad (2)$$

In this paper, we will use the well-known identity

$$wt(x \oplus y) = wt(x) + wt(y) - 2wt(x * y). \quad (3)$$

The cardinality of the set A is denoted by $|A|$. If $z = a + bi \in \mathbf{C}$, then $|z| = \sqrt{a^2 + b^2}$ denotes the absolute value of z and

$\bar{z} = a - bi$ denotes the complex conjugate of z , where $i^2 = -1$, $a, b \in \mathbf{R}$.

The Walsh-Hadamard transform of $f \in \mathcal{B}_n$ at any point $\omega \in F_2^n$ is denoted by

$$\mathcal{H}_f(\omega) = 2^{-n/2} \sum_{x \in F_2^n} (-1)^{f(x) \oplus \omega \cdot x}. \quad (4)$$

The nega-Hadamard transform of $f \in \mathcal{B}_n$ at any point $\omega \in F_2^n$ is the complex valued function:

$$\mathcal{NH}_f(\omega) = 2^{-n/2} \sum_{x \in F_2^n} (-1)^{f(x) \oplus \omega \cdot x} i^{wt(x)}. \quad (5)$$

A function $f \in \mathcal{B}_n$ is a bent function if $|\mathcal{H}_f(\omega)| = 1$ for all $\omega \in F_2^n$. Similarly, f is called negabent function if $|\mathcal{NH}_f(\omega)| = 1$ for all $\omega \in F_2^n$. It is interesting to note that all the affine functions (both odd and even) are negabent. If f is both bent and negabent, we say that f is bent-negabent. They will be interesting as they have extreme properties in terms of two different Fourier transforms.

The nega-cross-correlation coefficient of f and g at ω is denoted by

$$\mathcal{NC}_{f,g}(\omega) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus g(x \oplus \omega)} (-1)^{\omega \cdot x}. \quad (6)$$

We define the nega-autocorrelation coefficient of f at ω by

$$\mathcal{AC}_f(\omega) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus f(x \oplus \omega)} (-1)^{\omega \cdot x}. \quad (7)$$

Note that $\mathcal{NC}_{f,g}(\omega) = (-1)^{wt(\omega)} \mathcal{NC}_{g,f}(\omega)$. The functions f and g are said to have *complementary nega-autocorrelation* if for all nonzero $u \in F_2^n$

$$\mathcal{AC}_f(u) + \mathcal{AC}_g(u) = 0. \quad (8)$$

Definition 1. Let $f(x), g(x) \in \mathcal{B}_n$, and the *sum-of-squares* indicator of the nega-cross-correlation between $f(x)$ and $g(x)$ is defined by

$$\Delta_{f,g} = \sum_{\omega \in F_2^n} \mathcal{NC}_{f,g}^2(\omega). \quad (9)$$

If $f = g$, then $\Delta_{f,f}$ is called the *sum-of-squares* indicator of the nega-autocorrelation of f and denoted by Δ_f ; that is,

$$\Delta_f = \sum_{\omega \in F_2^n} \mathcal{AC}_f^2(\omega). \quad (10)$$

Note that $\mathcal{AC}_f(0) = 2^n$. Thus, $\Delta_f = \sum_{\omega \in F_2^n} \mathcal{AC}_f^2(\omega) \geq \mathcal{AC}_f^2(0) = 2^{2n}$. A Boolean function $f(x) \in \mathcal{B}_n$ is negabent if and only if $\mathcal{AC}_f(\omega) = 0$ for all $\omega \in F_2^n - \{0\}$. Hence, $\Delta_f \geq 2^{2n}$, where the equality holds if and only if f is negabent function.

3. Some Cryptographic Properties of Boolean Functions by Concatenation

In this section, we will use concatenation of Boolean functions. Let $f_1, f_2 \in \mathcal{B}_{n-1}$ and $f(x) \in \mathcal{B}_n$. We denote the

concatenation of f_1, f_2 by $f_1 \parallel f_2$. So, $f = f_1 \parallel f_2$ means that in algebraic normal form

$$f(x_1, x_2, \dots, x_n) = (1 \oplus x_n) f_1(x_1, x_2, \dots, x_{n-1}) \oplus x_n f_2(x_1, x_2, \dots, x_{n-1}). \quad (11)$$

The concatenation simply means that the truth tables of the functions are merged. For $f = f_1 \parallel f_2$, the upper half part of the truth table of f corresponds to f_1 and the lower half part to f_2 . The concatenation of affine functions together with certain nonlinear function has been used in several works [13–15].

In [6, 9], the function $h(\mathbf{x}, y) = f \parallel g = f(\mathbf{x})(1 \oplus y) \oplus g(\mathbf{x})y$ was studied and the following result was obtained.

Theorem 2 (see [6, 9]). Suppose $h \in \mathcal{B}_{n+1}$ is expressed as

$$h(\mathbf{x}, y) = f(\mathbf{x})(1 \oplus y) \oplus g(\mathbf{x})y \quad (12)$$

for all $(\mathbf{x}, y) \in \mathbb{F}_2^n \times \mathbb{F}_2$, where $f, g \in \mathcal{B}_n$. Then the following statements are equivalent.

- (i) h is negabent.
- (ii) f and g have complementary nega-autocorrelations and $\mathcal{N}\mathcal{C}_{f,g}(u) = 0$ for all $u \in \mathbb{F}_2^n$ with $\text{wt}(u) \equiv 1 \pmod{2}$.
- (iii) $|\mathcal{N}\mathcal{H}_f(u)|^2 + |\mathcal{N}\mathcal{H}_g(u)|^2 = 2$ for all $u \in \mathbb{F}_2^n$ and $\mathcal{N}\mathcal{H}_f(u)/\mathcal{N}\mathcal{H}_g(u)$ is a real number whenever $|\mathcal{N}\mathcal{H}_f(u)||\mathcal{N}\mathcal{H}_g(u)| \neq 0$.

In the following, we establish here a new equivalent statement. Also, we give an alternate proof of Theorem 13 [6, 9].

Theorem 3. Let $h \in \mathcal{B}_{n+1}$ be expressed as

$$h(\mathbf{x}, y) = f(\mathbf{x})(1 \oplus y) \oplus g(\mathbf{x})y \quad (13)$$

for all $(\mathbf{x}, y) \in \mathbb{F}_2^n \times \mathbb{F}_2$, where $f, g \in \mathcal{B}_n$. Then the following statements are equivalent.

- (1) h is negabent.
- (2) $|\mathcal{N}\mathcal{H}_f(u)|^2 + |\mathcal{N}\mathcal{H}_g(u)|^2 = 2$ for all $u \in \mathbb{F}_2^n$ and $\mathcal{N}\mathcal{H}_f(u)/\mathcal{N}\mathcal{H}_g(u)$ is a real number whenever $|\mathcal{N}\mathcal{H}_f(u)||\mathcal{N}\mathcal{H}_g(u)| \neq 0$.
- (3) f and g are negabent functions and

$$\begin{aligned} & (\mathcal{N}\mathcal{H}_f(u), \mathcal{N}\mathcal{H}_g(u)) \\ & \in \begin{cases} \{(\pm 1, \pm 1), (\pm i, \pm i)\}, & \text{if } n \text{ is even,} \\ \left\{ \left(\pm \frac{1+i}{\sqrt{2}}, \pm \frac{1+i}{\sqrt{2}} \right), \left(\pm \frac{1-i}{\sqrt{2}}, \pm \frac{1-i}{\sqrt{2}} \right) \right\}, & \text{if } n \text{ is odd,} \end{cases} \end{aligned} \quad (14)$$

where $u \in \mathbb{F}_2^n$.

Proof. We first show (1) \Rightarrow (2). By using the definition of the nega-Hadamard transform, we compute that

$$\begin{aligned} \mathcal{N}\mathcal{H}_h(\mathbf{u}, a) &= \begin{cases} \frac{1}{\sqrt{2}} \mathcal{N}\mathcal{H}_f(\mathbf{u}) + \frac{i}{\sqrt{2}} \mathcal{N}\mathcal{H}_g(\mathbf{u}), & \text{if } a = 0, \\ \frac{1}{\sqrt{2}} \mathcal{N}\mathcal{H}_f(\mathbf{u}) - \frac{i}{\sqrt{2}} \mathcal{N}\mathcal{H}_g(\mathbf{u}), & \text{if } a = 1. \end{cases} \end{aligned} \quad (15)$$

As h is negabent, $\mathcal{N}\mathcal{H}_h(\mathbf{u}, a) = 1$, we have

$$\begin{aligned} \left| \frac{1}{\sqrt{2}} \mathcal{N}\mathcal{H}_f(\mathbf{u}) + \frac{i}{\sqrt{2}} \mathcal{N}\mathcal{H}_g(\mathbf{u}) \right| &= 1, \\ \left| \frac{1}{\sqrt{2}} \mathcal{N}\mathcal{H}_f(\mathbf{u}) - \frac{i}{\sqrt{2}} \mathcal{N}\mathcal{H}_g(\mathbf{u}) \right| &= 1. \end{aligned} \quad (16)$$

According to (5), set

$$\begin{aligned} \mathcal{N}\mathcal{H}_f(u) &= 2^{-n/2} (a + bi), \\ \mathcal{N}\mathcal{H}_g(u) &= 2^{-n/2} (c + di), \end{aligned} \quad (17)$$

$$a, b, c, d \in \mathbb{Z}.$$

Hence,

$$\begin{aligned} |\mathcal{N}\mathcal{H}_f(u)| &= \sqrt{2^{-n} (a^2 + b^2)}, \\ |\mathcal{N}\mathcal{H}_g(u)| &= \sqrt{2^{-n} (c^2 + d^2)}, \\ \left| \frac{2^{-n/2}}{\sqrt{2}} (a - d) + \frac{2^{-n/2}}{\sqrt{2}} (b + c)i \right| &= 1, \\ \left| \frac{2^{-n/2}}{\sqrt{2}} (a + d) + \frac{2^{-n/2}}{\sqrt{2}} (b - c)i \right| &= 1; \end{aligned} \quad (18)$$

that is,

$$\begin{aligned} (a - d)^2 + (b + c)^2 &= 2^{n+1}, \\ (a + d)^2 + (b - c)^2 &= 2^{n+1}. \end{aligned} \quad (19)$$

From (19), we have

$$2^{-n} (a^2 + b^2) + 2^{-n} (c^2 + d^2) = 2, \quad ad = bc. \quad (20)$$

Thus, $|\mathcal{N}\mathcal{H}_f(u)|^2 + |\mathcal{N}\mathcal{H}_g(u)|^2 = 2$. Since $ad = bc$, suppose, for all $u \in \mathbb{F}_2^n$, $|\mathcal{N}\mathcal{H}_f(u)||\mathcal{N}\mathcal{H}_g(u)| \neq 0$; then

$$\begin{aligned} \frac{\mathcal{N}\mathcal{H}_f(u)}{\mathcal{N}\mathcal{H}_g(u)} &= \frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} \\ &= \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} \in \mathbb{R}. \end{aligned} \quad (21)$$

We now show (2) \Rightarrow (3). By (2), since $|\mathcal{N}\mathcal{H}_f(u)|^2 + |\mathcal{N}\mathcal{H}_g(u)|^2 = 2$ for all $u \in \mathbb{F}_2^n$, then

$$2^{-n} (a^2 + b^2 + c^2 + d^2) = 2; \quad (22)$$

that is,

$$a^2 + b^2 + c^2 + d^2 = 2^{n+1}. \quad (23)$$

Note that $a, b, c, d \in \mathbf{Z}$. There are two cases to be considered: n even and n odd.

Case 1 (n is even). By applying *Jacobi's four-square theorem*, (14) has exactly 24 solutions, which are all variations in \pm sign and order of $(\pm 2^{n/2}, \pm 2^{n/2}, 0, 0)$. Further, it is straightforward to check that, among these 24 solutions, the eight tuples (a, b, c, d) , in the list below, are also satisfying $\mathcal{NH}_f(u)/\mathcal{NH}_g(u)$ which is a real number whenever $|\mathcal{NH}_f(u)|, |\mathcal{NH}_g(u)| \neq 0$,

$$\begin{aligned} & (2^{(n-1)/2}, 2^{(n-1)/2}, 2^{(n-1)/2}, 2^{(n-1)/2}), (2^{(n-1)/2}, 2^{(n-1)/2}, -2^{(n-1)/2}, -2^{(n-1)/2}), \\ & (2^{(n-1)/2}, -2^{(n-1)/2}, -2^{(n-1)/2}, 2^{(n-1)/2}), (2^{(n-1)/2}, -2^{(n-1)/2}, 2^{(n-1)/2}, -2^{(n-1)/2}), \\ & (-2^{(n-1)/2}, 2^{(n-1)/2}, 2^{(n-1)/2}, -2^{(n-1)/2}), (-2^{(n-1)/2}, -2^{(n-1)/2}, 2^{(n-1)/2}, 2^{(n-1)/2}), \\ & (-2^{(n-1)/2}, 2^{(n-1)/2}, -2^{(n-1)/2}, 2^{(n-1)/2}), (-2^{(n-1)/2}, -2^{(n-1)/2}, -2^{(n-1)/2}, -2^{(n-1)/2}). \end{aligned} \quad (26)$$

Then,

$$\begin{aligned} & (\mathcal{NH}_f(u), \mathcal{NH}_g(u)) \\ & \in \left\{ \left(\pm \frac{1+i}{\sqrt{2}}, \pm \frac{1+i}{\sqrt{2}} \right), \left(\pm \frac{1-i}{\sqrt{2}}, \pm \frac{1-i}{\sqrt{2}} \right) \right\}. \end{aligned} \quad (27)$$

So, $|\mathcal{NH}_f(u)| = |\mathcal{NH}_g(u)| = 1$, where $u \in \mathbf{F}_2^n$.

Summarizing Cases 1 and 2, we conclude that f and g are negabent functions if (2) holds.

In the end, we show (3) \Rightarrow (1). According to (15), thanks to (14), (1) holds. This completes the proof. \square

In the following, for $f = f_1 \parallel f_2$, we discuss a connection among $\Delta_f, \Delta_{f_1}, \Delta_{f_2}$, and Δ_{f_1, f_2} . At first, according to the proof of Theorem 3 and Corollary 2 in [6, 9], we have the following.

Lemma 4 (see [6, 9]). *Let $f(x, x_n) = f_1 \parallel f_2 \in \mathcal{B}_n$, $x \in \mathbf{F}_2^{n-1}$, $x_n \in \mathbf{F}_2$, $f_1, f_2 \in \mathcal{B}_{n-1}$; then*

$$\begin{aligned} & \mathcal{NC}_f(\omega, \omega_n) \\ & = \begin{cases} \mathcal{NC}_{f_1}(\omega) + \mathcal{NC}_{f_2}(\omega), & \text{if } \omega_n = 0, \\ \mathcal{NC}_{f_1, f_2}(\omega) - (-1)^{wt(\omega)} \mathcal{NC}_{f_1, f_2}(\omega), & \text{if } \omega_n = 1, \end{cases} \end{aligned} \quad (28)$$

where $\omega \in \mathbf{F}_2^{n-1}$, $\omega_n \in \mathbf{F}_2$.

To obtain a connection among $\Delta_f, \Delta_{f_1}, \Delta_{f_2}$, and Δ_{f_1, f_2} , the following lemma is needed.

$$\begin{aligned} & (a, b, c, d) \\ & \in \{(\pm 2^{n/2}, 0, \pm 2^{n/2}, 0), (0, \pm 2^{n/2}, 0, \pm 2^{n/2})\}. \end{aligned} \quad (24)$$

Therefore,

$$(\mathcal{NH}_f(u), \mathcal{NH}_g(u)) \in \{(\pm 1, \pm 1), (\pm i, \pm i)\}. \quad (25)$$

So, $|\mathcal{NH}_f(u)| = |\mathcal{NH}_g(u)| = 1$, where $u \in \mathbf{F}_2^n$.

Case 2 (n is odd). Similarly, from *Jacobi's four-square theorem*, (14) has exactly 24 solutions, which are all variations in \pm sign and order of $(\pm 2^{(n+1)/2}, 0, 0, 0)$ or $(\pm 2^{(n-1)/2}, \pm 2^{(n-1)/2}, \pm 2^{(n-1)/2}, \pm 2^{(n-1)/2})$. Further, it is straightforward to check that, among these 24 solutions, the eight tuples (a, b, c, d) , in the list below, are also satisfying $\mathcal{NH}_f(u)/\mathcal{NH}_g(u)$ which is a real number whenever $|\mathcal{NH}_f(u)|, |\mathcal{NH}_g(u)| \neq 0$,

Lemma 5. *Let $f, g \in \mathcal{B}_n$. Then*

$$\Delta_{f, g} = \sum_{\alpha \in \mathbf{F}_2^n} \mathcal{NC}_{f, g}^2(\alpha) = \sum_{\omega \in \mathbf{F}_2^n} \mathcal{NC}_f(\omega) \mathcal{NC}_g(\omega). \quad (29)$$

Proof. According to the definition of nega-autocorrelation coefficient, we have

$$\begin{aligned} & \sum_{\omega \in \mathbf{F}_2^n} \mathcal{NC}_f(\omega) \mathcal{NC}_g(\omega) \\ & = \sum_{\omega \in \mathbf{F}_2^n} \left(\sum_{x \in \mathbf{F}_2^n} (-1)^{f(x) \oplus f(x \oplus \omega) \oplus \omega \cdot x} \right. \\ & \quad \cdot \sum_{y \in \mathbf{F}_2^n} (-1)^{g(y) \oplus g(y \oplus \omega) \oplus \omega \cdot y} \Big) = \sum_{x, y \in \mathbf{F}_2^n} (-1)^{f(x) \oplus g(y)} \\ & \quad \cdot \sum_{\omega \in \mathbf{F}_2^n} (-1)^{f(x \oplus \omega) \oplus g(y \oplus \omega) \oplus \omega \cdot (x \oplus y)} \\ & = \sum_{x, y \in \mathbf{F}_2^n} (-1)^{f(x) \oplus g(y) \oplus (x \oplus y) \cdot x} \\ & \quad \cdot \sum_{\omega \in \mathbf{F}_2^n} (-1)^{f(x \oplus \omega) \oplus g(y \oplus \omega) \oplus (x \oplus \omega) \cdot (x \oplus y)} \end{aligned}$$

$$\begin{aligned}
&= \sum_{x \in \mathbb{F}_2^n} \sum_{y \in \mathbb{F}_2^n} (-1)^{f(x) \oplus g(y) \oplus (x \oplus y) \cdot x} \mathcal{NC}_{f,g}(x \oplus y) \\
&= \sum_{\alpha \in \mathbb{F}_2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus g(x \oplus \alpha) \oplus \alpha \cdot x} \mathcal{NC}_{f,g}(\alpha) \\
&= \sum_{\alpha \in \mathbb{F}_2^n} \mathcal{NC}_{f,g}^2(\alpha) = \Delta_{f,g}.
\end{aligned} \tag{30}$$

□

Remark 6. If we use *Cauchy's inequality*

$$\left(\sum_i a_i b_i \right)^2 \leq \sum_i a_i^2 \sum_i b_i^2 \tag{31}$$

to the sum on the right-hand side of (29), we get

$$\begin{aligned}
\Delta_{f,g} &= \sum_{\alpha \in \mathbb{F}_2^n} \mathcal{NC}_{f,g}^2(\alpha) = \sum_{\omega \in \mathbb{F}_2^n} \mathcal{NC}_f(\omega) \mathcal{NC}_g(\omega) \\
&\leq \left(\sum_{\omega \in \mathbb{F}_2^n} \mathcal{NC}_f^2(\omega) \right)^{1/2} \left(\sum_{\omega \in \mathbb{F}_2^n} \mathcal{NC}_g^2(\omega) \right)^{1/2} \\
&= \Delta_f^{1/2} \Delta_g^{1/2} = \sqrt{\Delta_f \Delta_g};
\end{aligned} \tag{32}$$

that is, $\Delta_{f,g} \leq \sqrt{\Delta_f \Delta_g}$. From Lemmas 4 and 5, we get the following.

Theorem 7. Let $f(x, x_n) = f_1 \parallel f_2 \in \mathcal{B}_n$, $x \in \mathbb{F}_2^{n-1}$, $x_n \in \mathbb{F}_2$, $f_1, f_2 \in \mathcal{B}_{n-1}$. Then

$$\begin{aligned}
\Delta_f &= \Delta_{f_1} + \Delta_{f_2} + 4\Delta_{f_1, f_2} \\
&\quad - 2 \sum_{\omega \in \mathbb{F}_2^{n-1}} (-1)^{wt(\omega)} \mathcal{NC}_{f_1, f_2}^2(\omega).
\end{aligned} \tag{33}$$

Proof. Applying (28) and (29), we have

$$\begin{aligned}
\Delta_f &= \sum_{\omega \in \mathbb{F}_2^{n-1}, \omega_n \in \mathbb{F}_2} \mathcal{NC}_f(\omega, \omega_n)^2 \\
&= \sum_{\omega \in \mathbb{F}_2^{n-1}, \omega_n=0} \left(\mathcal{NC}_{f_1}(\omega) + \mathcal{NC}_{f_2}(\omega) \right)^2 \\
&\quad + \sum_{\omega \in \mathbb{F}_2^{n-1}, \omega_n=1} \left(\mathcal{NC}_{f_1, f_2}(\omega) \right. \\
&\quad \left. - (-1)^{wt(\omega)} \mathcal{NC}_{f_1, f_2}(\omega) \right)^2 = \sum_{\omega \in \mathbb{F}_2^{n-1}} \mathcal{NC}_{f_1}^2(\omega) \\
&\quad + \sum_{\omega \in \mathbb{F}_2^{n-1}} \mathcal{NC}_{f_2}^2(\omega) + 2 \sum_{\omega \in \mathbb{F}_2^{n-1}} \mathcal{NC}_{f_1}(\omega) \mathcal{NC}_{f_2}(\omega)
\end{aligned}$$

$$\begin{aligned}
&+ 2 \sum_{\omega \in \mathbb{F}_2^{n-1}} \mathcal{NC}_{f_1, f_2}^2(\omega) - 2 \sum_{\omega \in \mathbb{F}_2^{n-1}} (-1)^{wt(\omega)} \\
&\quad \cdot \mathcal{NC}_{f_1, f_2}^2(\omega) = \Delta_{f_1} + \Delta_{f_2} + 4\Delta_{f_1, f_2} \\
&\quad - 2 \sum_{\omega \in \mathbb{F}_2^{n-1}} (-1)^{wt(\omega)} \mathcal{NC}_{f_1, f_2}^2(\omega).
\end{aligned} \tag{34}$$

Theorem 7 gives the relationship among $\Delta_f, \Delta_{f_1}, \Delta_{f_2}$, and Δ_{f_1, f_2} . Furthermore, we have $\Delta_f \geq \Delta_{f_1} + \Delta_{f_2}$, where the equality holds if and only if $\mathcal{NC}_{f_1, f_2}(\omega) = 0$ for all $\omega \in \mathbb{F}_2^{n-1}$. By Lemma 4, we give a construction for generating negabent functions. □

Corollary 8. Let $f \in \mathcal{B}_{n-1}$. Then $g \in \mathcal{B}_n = f \parallel \bar{f}$ is negabent if and only if f is also negabent functions, where the notation \bar{f} denotes the complement function of f ; that is, $\bar{f} = f \oplus 1$.

Proof. Using (15), for any $\omega \in \mathbb{F}_2^{n-1}$, $\omega_n \in \mathbb{F}_2$, we have

$$\begin{aligned}
&\mathcal{NH}_g(\omega, \omega_n) \\
&= \begin{cases} \frac{1}{\sqrt{2}} \mathcal{NH}_f(\omega) - \frac{i}{\sqrt{2}} \mathcal{NH}_f(\omega), & \text{if } \omega_n = 0, \\ \frac{1}{\sqrt{2}} \mathcal{NH}_f(\omega) + \frac{i}{\sqrt{2}} \mathcal{NH}_f(\omega), & \text{if } \omega_n = 1, \end{cases} \\
&= \left(\frac{1}{\sqrt{2}} \mp \frac{i}{\sqrt{2}} \right) \mathcal{NH}_f(\omega).
\end{aligned} \tag{35}$$

Hence

$$|\mathcal{NH}_g(\omega)| = \left| \frac{1}{\sqrt{2}} \mp \frac{i}{\sqrt{2}} \right| |\mathcal{NH}_f(\omega)| = |\mathcal{NH}_f(\omega)|. \tag{36}$$

Since f is negabent, $|\mathcal{NH}_f(\omega)| = 1$ for all $\omega_n \in \mathbb{F}_2$, completing the proof. □

There are many ways to construct bent functions in \mathcal{B}_{m+n} starting from bent functions in \mathcal{B}_m and \mathcal{B}_n (see [16, pages 81–96]). Concatenation under certain conditions produces also bent functions of higher dimension (see [15]). In the following, we mainly consider Boolean function

$$\begin{aligned}
g(x, x_{n+1}, x_{n+2}) &= f_1(x) \parallel f_2(x) \parallel f_3(x) \parallel f_4(x) \\
&\in \mathcal{B}_{n+2};
\end{aligned} \tag{37}$$

that is, the algebraic normal form of $g(x, x_{n+1}, x_{n+2})$ is

$$\begin{aligned}
g(x, x_{n+1}, x_{n+2}) &= f_1 \oplus x_{n+1} (f_1 \oplus f_2) \\
&\quad \oplus x_{n+2} (f_1 \oplus f_3) \\
&\quad \oplus x_{n+1} x_{n+2} (f_1 \oplus f_2 \oplus f_3 \oplus f_4),
\end{aligned} \tag{38}$$

where $f_i \in \mathcal{B}_n$, $i = 1, 2, 3, 4$, $x \in \mathbb{F}_2^n$, $x_{n+1}, x_{n+2} \in \mathbb{F}_2$. We first establish an important technical formula.

Theorem 9. Let function g be defined as (37); then

$$\begin{aligned} \mathcal{NH}_g(\omega) &= \frac{1}{2} \left[\mathcal{NH}_{f_1}(u) + i(-1)^a \mathcal{NH}_{f_2}(u) \right. \\ &\quad \left. + i(-1)^b \mathcal{NH}_{f_3}(u) - (-1)^{a \oplus b} \mathcal{NH}_{f_4}(u) \right], \end{aligned} \quad (39)$$

where $\omega = (u, a, b) \in F_2^{n+2}$, $u \in F_2^n$, $a, b \in F_2$.

Proof. Using (5), we have

$$\begin{aligned} \mathcal{NH}_g(\omega) &= 2^{-(n+2)/2} \sum_{(x, x_{n+1}, x_{n+2}) \in F_2^{n+2}} (-1)^{g(x, x_{n+1}, x_{n+2}) \oplus (x, x_{n+1}, x_{n+2}) \cdot \omega} \\ &\quad \cdot i^{wt(x, x_{n+1}, x_{n+2})} = \frac{1}{2} \\ &\quad \cdot 2^{-n/2} \sum_{(x, x_{n+1}, x_{n+2}) \in F_2^{n+2}} (-1)^{g(x, x_{n+1}, x_{n+2}) \oplus u \cdot x \oplus a x_{n+1} \oplus b x_{n+2}} \\ &\quad \cdot i^{wt(x, x_{n+1}, x_{n+2})} = \frac{1}{2} \\ &\quad \cdot 2^{-n/2} \sum_{x \in F_2^n} \sum_{(x_{n+1}, x_{n+2}) \in F_2^2} (-1)^{g(x, x_{n+1}, x_{n+2}) \oplus u \cdot x \oplus a x_{n+1} \oplus b x_{n+2}} \\ &\quad \cdot i^{wt(x, x_{n+1}, x_{n+2})} = \frac{1}{2} \cdot 2^{-n/2} \left[\sum_{x \in F_2^n} (-1)^{f_1(x) \oplus u \cdot x} i^{wt(x)} \right. \\ &\quad + \sum_{x \in F_2^n} (-1)^{f_2(x) \oplus u \cdot x \oplus a} i^{wt(x)+1} + \sum_{x \in F_2^n} (-1)^{f_3(x) \oplus u \cdot x \oplus b} \\ &\quad \cdot i^{wt(x)+1} + \sum_{x \in F_2^n} (-1)^{f_4(x) \oplus u \cdot x \oplus a \oplus b} i^{wt(x)+2} \left. \right] \\ &= \frac{1}{2} \left[\mathcal{NH}_{f_1}(u) + i(-1)^a \mathcal{NH}_{f_2}(u) + i(-1)^b \right. \\ &\quad \cdot \mathcal{NH}_{f_3}(u) - (-1)^{a \oplus b} \mathcal{NH}_{f_4}(u) \left. \right]. \end{aligned} \quad (40)$$

This completes the proof. \square

In (37), if $f_1 = f_4 = f$, $f_2 = f_3 = \bar{f}$, then we obtain the following.

Corollary 10. Let $f \in \mathcal{B}_n$. Then $g \in \mathcal{B}_{n+2} = f \parallel \bar{f} \parallel \bar{f} \parallel f$ is negabent if and only if f is also negabent functions.

Proof. According to (39), we have

$$\begin{aligned} \mathcal{NH}_g(u, a, b) &= \frac{1 - (-1)^{a \oplus b}}{2} \mathcal{NH}_f(u) \\ &\quad - i \frac{(-1)^a + (-1)^b}{2} \mathcal{NH}_f(u) \end{aligned}$$

$$= \begin{cases} -i \mathcal{NH}_f(u), & a = 0, b = 0, \\ \mathcal{NH}_f(u), & a = 0, b = 1, \\ \mathcal{NH}_f(u), & a = 1, b = 0, \\ i \mathcal{NH}_f(u), & a = 1, b = 1. \end{cases} \quad (41)$$

Thus, $\mathcal{NH}_g(u, a, b) \in \{\mathcal{NH}_f(u), \pm i \mathcal{NH}_f(u)\}$ for all $(u, a, b) \in F_2^n \times F_2 \times F_2$. Hence, if g is negabent, then f is also negabent. Conversely, if f is negabent, then g is also negabent, completing the proof. \square

4. Nega-Hadamard Transform and Nega-Autocorrelation Coefficients of a Class of Boolean Function

In this section, we mainly study the function $g(x) \in \mathcal{B}_n$ expressed as

$$g(x) = f(Ax \oplus a) \oplus b \cdot x \oplus c, \quad (42)$$

where $f(x) \in \mathcal{B}_n$, $a, b \in F_2^n$, $c \in F_2$, and A is an $n \times n$ orthogonal matrix. Here we compute the nega-Hadamard transform and nega-autocorrelation coefficient of g .

Theorem 11. Let $g \in \mathcal{B}_n$, with the same data as above; then

$$\begin{aligned} \mathcal{NH}_g(\omega) &= (-1)^{c \oplus A(b \oplus \omega) \cdot a} i^{wt(a)} \mathcal{NH}_f(A(b \oplus \omega) \oplus a), \end{aligned} \quad (43)$$

$$\mathcal{NC}_g(\alpha) = (-1)^{(A^T a \oplus b) \cdot \alpha} \mathcal{NC}_f(A\alpha). \quad (44)$$

Proof. According to (5), we have

$$\begin{aligned} \mathcal{NH}_g(\omega) &= 2^{-n/2} \sum_{x \in F_2^n} (-1)^{f(Ax \oplus a) \oplus b \cdot x \oplus c \oplus \omega \cdot x} i^{wt(x)} \\ &= (-1)^c 2^{-n/2} \sum_{x \in F_2^n} (-1)^{f(Ax \oplus a) \oplus (b \oplus \omega) \cdot x} i^{wt(x)}. \end{aligned} \quad (45)$$

Setting $y = Ax \oplus a$, since A is orthogonal matrix, then $A^T A = AA^T = I$, where A^T is the transpose of A and I is the identity matrix; then $x = A^T(y \oplus a)$. Furthermore, when x ranges over F_2^n , so do Ax and $Ax \oplus a$. Thus

$$\begin{aligned} \mathcal{NH}_g(\omega) &= (-1)^c \\ &\quad \cdot 2^{-n/2} \sum_{y \in F_2^n} (-1)^{f(y) \oplus (b \oplus \omega) \cdot (A^T y + A^T a)} i^{wt(A^T(y \oplus a))} \\ &= (-1)^{c \oplus (b \oplus \omega) \cdot A^T a} \\ &\quad \cdot 2^{-n/2} \sum_{y \in F_2^n} (-1)^{f(y) \oplus (b \oplus \omega) \cdot A^T y} i^{wt(A^T(y \oplus a))} \\ &= (-1)^{c \oplus A(b \oplus \omega) \cdot a} \\ &\quad \cdot 2^{-n/2} \sum_{y \in F_2^n} (-1)^{f(y) \oplus A(b \oplus \omega) \cdot y} i^{wt(A^T(y \oplus a))}. \end{aligned} \quad (46)$$

Since

$$\begin{aligned}
 wt(A^T(y \oplus a)) &= (A^T(y \oplus a))^T I(A^T(y \oplus a)) \\
 &= (y \oplus a)^T A I A^T(y \oplus a) \\
 &= (y \oplus a)^T I(y \oplus a) = wt(y \oplus a), \\
 i^{wt(y \oplus a)} &= i^{wt(y) + wt(a) - 2wt(y * a)} \\
 &= i^{wt(y) + wt(a)} i^{-2wt(y * a)} \\
 &= i^{wt(y) + wt(a)} (-1)^{-wt(y * a)} \\
 &= i^{wt(y) + wt(a)} (-1)^{wt(y * a)} \\
 &= i^{wt(y) + wt(a)} (-1)^{y \cdot a},
 \end{aligned} \tag{47}$$

which implies that

$$\begin{aligned}
 \mathcal{NH}_g(\omega) &= (-1)^{c \oplus A(b \oplus \omega) \cdot a} 2^{-n/2} \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y) \oplus A(b \oplus \omega) \cdot y} \\
 &\cdot i^{wt(y \oplus a)} = (-1)^{c \oplus A(b \oplus \omega) \cdot a} \\
 &\cdot 2^{-n/2} \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y) \oplus A(b \oplus \omega) \cdot y} i^{wt(y) + wt(a)} (-1)^{y \cdot a} \\
 &= (-1)^{c \oplus A(b \oplus \omega) \cdot a} \\
 &\cdot i^{wt(a)} 2^{-n/2} \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y) \oplus (A(b \oplus \omega) \oplus a) \cdot y} i^{wt(y)} \\
 &= (-1)^{c \oplus A(b \oplus \omega) \cdot a} i^{wt(a)} \mathcal{NH}_f(A(b \oplus \omega) \oplus a).
 \end{aligned} \tag{48}$$

Thus (43) holds. Next we will compute (44). Set

$$\begin{aligned}
 h(x) &= g(x) \oplus g(x \oplus \alpha) \oplus \alpha \cdot x \\
 &= f(Ax \oplus a) \oplus b \cdot x \oplus c \oplus f(A(x \oplus \alpha) \oplus a) \oplus b \\
 &\cdot (x \oplus \alpha) \oplus c \oplus \alpha \cdot x \\
 &= f(Ax \oplus a) \oplus f(Ax \oplus A\alpha \oplus a) \oplus b \cdot \alpha \oplus \alpha \cdot x.
 \end{aligned} \tag{49}$$

So by using (6), we get

$$\begin{aligned}
 \mathcal{NE}_g(\alpha) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{g(x) \oplus g(x \oplus \alpha) \oplus \alpha \cdot x} \\
 &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(Ax \oplus a) \oplus f(Ax \oplus A\alpha \oplus a) \oplus b \cdot \alpha \oplus \alpha \cdot x} \\
 &= (-1)^{b \cdot \alpha} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(Ax \oplus a) \oplus f(Ax \oplus A\alpha \oplus a) \oplus \alpha \cdot x}.
 \end{aligned} \tag{50}$$

Setting $y = Ax \oplus a$, as A is orthogonal matrix, then $x = A^T(y \oplus a) = A^T y \oplus A^T a$. Therefore,

$$\begin{aligned}
 \mathcal{NE}_g(\alpha) &= (-1)^{b \cdot \alpha} \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y) \oplus f(y \oplus A\alpha) \oplus \alpha \cdot (A^T y \oplus A^T a)} \\
 &= (-1)^{(A^T a \oplus b) \cdot \alpha} \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y) \oplus f(y \oplus A\alpha) \oplus \alpha \cdot A^T y} \\
 &= (-1)^{(A^T a \oplus b) \cdot \alpha} \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y) \oplus f(y \oplus A\alpha) \oplus A\alpha \cdot y} \\
 &= (-1)^{(A^T a \oplus b) \cdot \alpha} \mathcal{NE}_f(A\alpha).
 \end{aligned} \tag{51}$$

This completes the proof. \square

By Theorem 11, we can easily get the following results proved in [6, 9, Theorem 1 (a) and (d)].

Corollary 12. Let $f(x) \in \mathcal{B}_n$; then one obtains the following.

- (a) Consider $\mathcal{NH}_{\bar{f}}(\omega) = -\mathcal{NH}_f(\omega)$, $\omega \in \mathbb{F}_2^n$.
- (b) If $g(x) = f(Ax \oplus a)$, then $\mathcal{NH}_g(\omega) = (-1)^{A\omega \cdot a} i^{wt(a)} \mathcal{NH}_f(A\omega \oplus a)$, where A is an $n \times n$ orthogonal matrix, $a \in \mathbb{F}_2^n$.

It is known that if $f(x)$ is a bent function in (42), then the function $g(x)$ is also bent, where A is an $n \times n$ nonsingular matrix. The Boolean function $f(x) \in \mathcal{B}_n$ is a negabent function if $|\mathcal{NH}_f(\omega)| = 1$. Therefore, according to (43), we get that if $f(x)$ is a negabent function, then g is also negabent. The following result summarizes this discussion.

Corollary 13. With the same data as in Theorem 3, then if $f(x)$ is bent-negabent, $g(x)$ is also bent-negabent.

In (42), by choosing some special cases and Corollary 13, we have the following.

Corollary 14. Let $f(x) \in \mathcal{B}_n$ be a bent-negabent function; then one obtains the following.

- (a) $f_1(x) = f(x \oplus \omega)$ is bent-negabent, where $\omega \in \mathbb{F}_2^n$.
- (b) $f_2(x) = f(x) \oplus a \cdot x \oplus b$ is bent-negabent, where $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2$.

Remark 15. Corollary 12 was mentioned in [3, Lemma 2], and Corollary 10 was proved in [4, Theorem 2] by applying [3, Lemma 2]. However, if we use Theorem 11, these results are easily obtained.

5. Conclusion

In this paper, the special Boolean functions by concatenation are presented. We investigate their nega-Hadamard transforms, nega-autocorrelation coefficients, sum-of-squares indicators, and so on. We establish a new equivalent statement on $f_1 \parallel f_2$ which is negabent function. Also, we give an alternate proof of Theorem 13 [6, 9]. Based on them,

the construction for generating the negabent functions by concatenation is given. Finally, the function expressed as $f(Ax \oplus a) \oplus b \cdot x \oplus c$ is discussed. The nega-Hadamard transform and nega-autocorrelation coefficient of this function are derived. By applying these results, some properties are obtained. We hope that these results will be helpful in further studying of Boolean functions.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work was supported by the Natural Science Foundation of Anhui Higher Education Institutions of China (nos. KJ2014A220 and KJ2014A231).

References

- [1] O. S. Rothaus, "On 'bent' functions," *Journal of Combinatorial Theory, Series A*, vol. 20, no. 3, pp. 300–305, 1976.
- [2] C. Riera and M. G. Parker, "Generalized bent criteria for Boolean functions (I)," *IEEE Transactions on Information Theory*, vol. 52, no. 9, pp. 4142–4159, 2006.
- [3] M. G. Parker and A. Pott, "On Boolean functions which are bent and negabent," in *Sequences, Subsequences, and Consequences*, S. W. Golomb, G. Gong, T. Helleseth, and H.-Y. Song, Eds., vol. 4893 of *Lecture Notes in Computer Science*, pp. 9–23, Springer, Berlin, Germany, 2007.
- [4] K. U. Schmidt, M. G. Parker, and A. Pott, "Negabent functions in the Maiorana-McFarland class," in *Sequences and Their Applications—SETA 2008*, S. W. Golomb, M. G. Parker, A. Pott, and A. Winterof, Eds., vol. 5203 of *Lecture Notes in Computer Science*, pp. 390–402, Springer, Berlin, Germany, 2008.
- [5] S. Sarkar, "On the symmetric negabent Boolean functions," in *Progress in Cryptology—INDOCRYPT 2009*, B. Roy and N. Sendrier, Eds., vol. 5922 of *Lecture Notes in Computer Science*, pp. 136–143, Springer, Berlin, Germany, 2009.
- [6] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A. K. Gangopadhyay, and S. Maitra, "Nega-Hadamard transform, bent and negabent functions," in *Sequences and Their Applications—SETA 2010*, C. Carlet and A. Pott, Eds., vol. 6338 of *Lecture Notes in Computer Science*, pp. 359–372, Springer, Berlin, Germany, 2010.
- [7] S. Gangopadhyay and A. Chaturvedi, "A new class of bent-negabent Boolean Functions," <http://eprint.iacr.org/2010/597.pdf>.
- [8] S. Sarkar, "Characterizing negabent Boolean functions over finite fields," in *Sequences and Their Applications—SETA 2012*, T. Helleseth and J. Jedwab, Eds., vol. 7280 of *Lecture Notes in Computer Science*, pp. 77–88, Springer, Berlin, Germany, 2012.
- [9] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A. K. Gangopadhyay, and S. Maitra, "Investigations on bent and negabent functions via the Nega-Hadamard transform," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 4064–4072, 2012.
- [10] W. Su, A. Pott, and X. Tang, "Characterization of negabent functions and construction of bent-negabent functions with maximum algebraic degree," *IEEE Transactions on Information Theory*, vol. 59, no. 6, pp. 3387–3395, 2013.
- [11] F. Zhang, Y. Wei, and E. Pasalic, "Constructions of bent—negabent functions and their relation to the completed Maiorana—McFarland class," *IEEE Transactions on Information Theory*, vol. 61, no. 3, pp. 1496–1506, 2015.
- [12] C. Carlet, "On the secondary constructions of resilient and bent functions," in *Coding, Cryptography and Combinatorics*, vol. 23 of *Progress in Computer Science and Applied Logic*, pp. 3–28, Birkhäuser, Basel, Switzerland, 2004.
- [13] W. Zhang and G. Xiao, "Constructions of almost optimal resilient Boolean functions on large even number of variables," *IEEE Transactions on Information Theory*, vol. 55, no. 12, pp. 5822–5831, 2009.
- [14] W.-G. Zhang and E. Pasalic, "Constructions of resilient S-boxes with strictly almost optimal nonlinearity through disjoint linear codes," *IEEE Transactions on Information Theory*, vol. 60, no. 3, pp. 1638–1651, 2014.
- [15] B. Preneel, W. V. Leekwijck, L. V. Linden et al., "Propagation characteristics of Boolean functions," in *Advances in Cryptology—EUROCRYPT '90*, vol. 473 of *Lecture Notes in Computer Science*, pp. 161–173, Springer, Berlin, Germany, 1991.
- [16] T. W. Cusick and P. Stănică, *Cryptographic Boolean Functions and Applications*, Elsevier-Academic Press, 2009.

