Weightwise perfectly balanced functions with high weightwise nonlinearity profile

Jian Liu1,2 · Sihem Mesnager3,4

Received: 22 February 2018 / Revised: 23 June 2018 / Accepted: 30 October 2018 / Published online: 10 November 2018 © Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract
Boolean functions satisfying good cryptographic criteria when restricted to the set of vectors with constant Hamming weight play an important role in the recent FLIP stream cipher (Méaux et al.: in Lecture Notes in Computer Science, vol. 9665, pp. 311–343, Springer, Berlin, 2016). In this paper, we propose a large class of weightwise perfectly balanced (WPB) functions, which is 2-rotation symmetric. This new class of WPB functions is not extended affinely equivalent to the known constructions. We also discuss the weightwise nonlinearity profile of these functions, and present general lower bounds on $k$-weightwise nonlinearity, where $k$ is a power of 2. Moreover, we exhibit a subclass of the family. By a recursive lower bound, we show that these subclass of WPB functions have very high weightwise nonlinearity profile.

Keywords FLIP cipher · Boolean function · Weightwise perfectly balanced · Weightwise nonlinearity

Mathematics Subject Classification 11T71 · 94A60 · 06E30

1 Introduction

Boolean functions used as primitives in stream ciphers and block ciphers are classically studied with input defined on the whole vector space $\mathbb{F}_2^n$. At Eurocrypt 2016, Méaux et al.
proposed a new family of stream ciphers, called FLIP, which is intended to be combined with a homomorphic encryption scheme to create an acceptable system of fully homomorphic encryption. The symmetric primitive FLIP requires the Hamming weight of the key register to be invariant. This produces a special situation for the structure of filter function: the input of the filter function consists of those vectors in $\mathbb{F}_2^n$ which have constant Hamming weight. Then, it leads to the problem on how to evaluate the security of a Boolean function with restricted input, i.e., the input of $f$ is a subset of $\mathbb{F}_2^n$. Besides, in particular stream ciphers, knowing the Hamming weight of a key register enables the attacker to distinguish the keystream from a random bit-stream [12]. Therefore, filter functions which have small bias when restricted to constant weight vectors are preferred.

Early studies on Boolean functions with input restricted to constant weight vectors can be found in [7–10]. Their work is asymptotical and from a probability point of view. In 2017, Carlet, Méaux, and Rotella [4] provided a security analysis on FLIP cipher and gave the first study on cryptographic criteria of Boolean functions with restricted input. An early version of FLIP faces an attack given by Duval et al. [6], which leads the design of the filter function to become more complicated in order to reach better criteria on the subsets of $\mathbb{F}_2^n$. For Boolean functions, the parameters balancedness and nonlinearity are strongly related to the resistance against distinguishing attack and affine approximation attack, respectively. In [4], it is shown that, for Boolean functions with restricted input, balancedness and nonlinearity parameters continue to play an important role with respect to the corresponding attacks on the framework of FLIP ciphers. In particular, Boolean functions which are uniformly distributed over $\{0, 1\}$ on $E_{n,k} = \{x \in \mathbb{F}_2^n \mid w_H(x) = k\}$ for every $0 < k < n$ are called weightwise perfectly balanced (WPB) functions, where $w_H(x)$ denotes the Hamming weight of $x$. The minimum Hamming distance between a Boolean function $f$ and all the affine Boolean functions is called the nonlinearity of $f$. If the input of $f$ is restricted to $E_{n,k}$, then the nonlinearity is called $k$-weight nonlinearity. The set of $k$-weight nonlinearity for all $0 < k < n$ is called the weightwise nonlinearity profile of $f$. To our best knowledge, the only known construction of WPB functions is due to [4], which is designed through a recursive method. Some upper bounds on the $k$-weight nonlinearity of Boolean functions are discussed in [4,17], respectively. As far as we know, there is no known construction of WPB functions which has high weightwise nonlinearity profile simultaneously.

In this paper, we focus on the constructions of WPB functions. We first propose a large family of WPB functions by presenting the trace form as well as the algebraic normal form. These WPB functions belong to generalized rotation symmetric Boolean functions [14], which also have potential applications in coding theory and S-box design [13,18]. Compared with the construction given by Carlet et al. [4], our family has a larger algebraic degree and is thus not extended affinely (EA) equivalent to the known ones. Afterwards, we discuss the weightwise nonlinearity of these WPB functions, showing that for every $k$ being a positive power of 2, the $k$-weightwise nonlinearity of any WPB function in our family is nonzero. Furthermore, we construct a subclass of WPB functions in our family, which have high $k$-weightwise nonlinearity for every $k > 1$. This is the first time that an infinite class of WPB functions with high weightwise nonlinearity profile has been constructed.

The remainder of this paper is organized as follows. Formal definitions and necessary preliminaries are introduced in Sect. 2. In Sect. 3, a family of WPB functions is proposed, and the analysis of the weightwise nonlinearity is presented. We exhibit a subclass of WPB functions with high weightwise nonlinearity profile in Sect. 4. Finally, we conclude the paper in Sect. 5.
2 Preliminaries

2.1 Boolean functions with restricted input

In this paper, additions and multiple sums calculated modulo 2 will be denoted by $\oplus$ and $\bigoplus$ respectively, additions and multiple sums calculated in characteristic 0 or in the additions of elements of the finite field $F_2$ will be denoted by $+$ and $\sum_i$ respectively. Let $F_n$ denote the $n$-dimensional vector space over the finite field $F_2$ with two elements. An $n$-variable Boolean function $f$ is a function from $F_n^m$ to $F_2$. The $(0, 1)$-sequence defined by $(f(v_0), f(v_1), \ldots, f(v_{2^n-1}))$ is called the truth table of $f$, where $v_0 = (0, \ldots, 0, 0), v_1 = (0, \ldots, 0, 1), v_2 = (0, \ldots, 1, 0), v_3 = (0, \ldots, 1, 1), \ldots, v_{2^n-1} = (1, \ldots, 1, 1)$ are ordered by lexicographical order. $f$ can be uniquely represented in the algebraic normal form (in brief, ANF) that

$$f(x) = \bigoplus_{v \in F_n^m} a_v x^v,$$

where the coefficient $a_v \in F_2$, $x^v = x_1^{v_1}x_2^{v_2} \cdots x_n^{v_n}$ for $x = (x_1, \ldots, x_n) \in F_n^m$ and $v = (v_1, \ldots, v_n) \in F_n^m$. The algebraic degree of $f$, denoted by $\deg(f)$, is the number of variables in the highest order product term with nonzero coefficient. A Boolean function is said to be affine if $\deg(f) \leq 1$, i.e., $f(x) = a \cdot x + c, a \in F_2^n, c \in F_2$, where $a \cdot x$ is the usual inner product defined as $a \cdot x = a_1x_1 \oplus \cdots \oplus a_nx_n$ for $a = (a_1, \ldots, a_n) \in F_2^n$ and $x = (x_1, \ldots, x_n) \in F_n^n$. Two Boolean functions $f$ and $g$ are said to be extended affinely (EA) equivalent if there exist an affine Boolean function $l$ and an affine automorphism $L$ of $F_2^n$ such that $f = g \circ L \oplus l$. The algebraic degree of an $n$-variable Boolean function $f$ is affine invariant, i.e., for every affine Boolean function $l$ and every affine automorphism $L$ of $F_2^n$, we have $\deg(f \circ L \oplus l) = \deg(f)$ (see [1]). Given a basis of $F_{2^n}$ over $F_2, F_{2^n}$ can be regarded as a vector space over $F_2$, and there is a bijective $F_2$-linear mapping from $F_{2^n}$ to $F_{2^n}$. Thus, the field $F_{2^n}$ can be identified with $F_{2^n}^2$. For simplicity, we do not distinguish elements in $F_{2^n}$ and in $F_{2^n}$ if the context is clear.

Recall that the cyclotomic classes of 2 modulo $2^n - 1$ are defined as $C(j) := \{j 2^i \mod (2^n - 1) \mid i = 0, 1, \ldots, o(j)\}$, where $o(j)$ is the smallest positive integer such that $j 2^{o(j)} \equiv j \mod (2^n - 1)$. For any positive integers $k$ and $r$ satisfying $r | k$, the trace function from $F_{2^{2k}}$ to $F_{2^r}$, denoted by $Tr_{2^r}^{2^k}$, is defined as $Tr_{2^r}^{2^k}(x) := x + x^{2^r} + x^{2^{2r}} + \cdots + x^{2^{k(r-1)}}$, $x \in F_{2^i}$. Through the choice of a basis of the vector space $F_{2^n}$, a Boolean function over $F_{2^n}$ can be uniquely represented in the following trace form [2]:

$$f(x) = \sum_{j \in \Gamma_n} Tr_{1}^{o(j)}(a_j x_j) + \epsilon \left(1 + x^{2^n-1}\right),$$

where $\Gamma_n$ is the set of all the coset leaders of the cyclotomic classes of 2 modulo $2^n - 1$, $o(j)$ is the size of the cyclotomic class of 2 modulo $2^n - 1$ containing $j, a_j \in F_{2(2^n)}, \epsilon = w_H(f) \mod 2, \text{ and } w_H(f) = |\{x \in F_{2^n} \mid f(x) = 1\}|$. The algebraic degree of $f$ in the above trace form is preserved, which can be read as $\deg(f) = \max\{w_{2^n}(j) \mid a_j \neq 0\}$ (we make $\epsilon = a_{2^n-1}$), where $w_{2^n}(j)$ is the number of nonzero coefficients $j_s$ in the binary expansion $\sum_{s = 0}^{n-1} j_s 2^s$ of $j$. Thus, all the affine Boolean functions have the form $Tr_{1}^{o}(ax) + c$, where $c \in F_2$ and $a \in F_{2^n}$.

Denote by $w_H(f)_k$ the Hamming weight of a Boolean function $f$ on all the entries with fixed Hamming weight $k$, i.e.,

$$w_H(f)_k = |\{x \in F_{2^n} \mid w_H(x) = k, f(x) = 1\}|.$$
where \( w_H \) denotes the Hamming weight of a vector.

**Definition 2.1** [4] For an \( n \)-variable Boolean function \( f \), \( f \) is called weightwise perfectly balanced (WPB) if for every \( k \in \{1, \ldots, n-1\} \), the restriction of \( f \) with input ranging over \( E_{n,k} = \{ x \in \mathbb{F}_2^n \mid w_H(x) = k \} \) is balanced, i.e., \( w_H(f)_k = \binom{n}{k}/2 \).

**Remark 2.2** For a WPB function \( f \), it is imposed that \( f(0, \ldots, 0) \neq f(1, \ldots, 1) \) to make the whole function balanced on \( \mathbb{F}_2^n \). Without loss of generality, we suppose that \( f(0, \ldots, 0) = 0 \) and \( f(1, \ldots, 1) = 1 \).

It is proved that weightwise perfectly balanced Boolean functions exist only if \( n \) is a power of 2 (see [4]). In this paper, we always consider Boolean functions with \( n = 2^k \) variables, where \( k \) is a positive integer.

Let \( E \) be a subset of \( \mathbb{F}_2^n \) and \( f \) be a Boolean function restricted on \( E \). The nonlinearity of \( f \) over \( E \), denoted by \( \text{NL}_E(f) \), is the minimum Hamming distance between \( f \) and all the affine functions, say \( a \cdot x \oplus c, a \in \mathbb{F}_2^n, c \in \mathbb{F}_2 \), restricted to \( E \). In particular, the set \( \{\text{NL}_{E_{n,k}}(f) \mid k = 1, \ldots, n-1\} \) is called the weightwise nonlinearity profile of \( f \), where \( E_{n,k} = \{ x \in \mathbb{F}_2^n \mid w_H(x) = k \} \). The value \( \text{NL}_{E_{n,k}}(f) \) is called the \( k \)-weight nonlinearity of \( f \), and will be denoted by \( \text{NL}_k(f) \) if there is no risk of confusion. The nonlinearity of \( f \) over a subset can be calculated as follows.

**Proposition 2.3** [4] Let \( f \) be an \( n \)-variable Boolean function and \( E \) be a subset of \( \mathbb{F}_2^n \). We have

\[
\text{NL}_E(f) = \frac{|E|}{2} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \left| \sum_{x \in E} (-1)^{f(x) \oplus a \cdot x} \right|.
\]

In [4], an upper bound on the nonlinearity of Boolean functions with restricted input is given. Mesnager [17] presented further advances on this upper bound, and stressed that the improved upper bound might be much lower than that in [4].

**Proposition 2.4** [4] Let \( f \) be an \( n \)-variable Boolean function, and \( \lfloor a \rfloor \) denote the maximum integer not larger than \( a \). Then, for every \( E \subseteq \mathbb{F}_2^n \), we have

\[
\text{NL}_E(f) \leq \left\lfloor \frac{|E|}{2} - \frac{\sqrt{|E|}}{2} \right\rfloor.
\]

### 2.2 Generalized rotation symmetric Boolean functions

For \( x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n \) and \( 0 \leq s \leq n-1 \), define the left \( s \)-cyclic shift operator \( \rho^s_n \) as

\[
\rho^s_n(x) = (x_{1+s}, x_{2+s}, \ldots, x_{n+s}),
\]

where for \( i = 1, \ldots, n, i+s \) takes the value \((i+s) \mod n\) with the only exception that \((i+s) = n\), which will be assigned by \( n \) instead of 0. If we choose a normal basis \( \{ \alpha, \alpha^2, \ldots, \alpha^{2^{n-1}} \} \) of the finite field \( \mathbb{F}_{2^n} \), and decompose \( x = x_1\alpha^{2^{n-1}} + x_2\alpha^{2^{n-2}} + \cdots + x_n\alpha = (x_1, \ldots, x_n) \in \mathbb{F}_2^n \) over this basis, then \( \rho^1_n(x) = x^2 \), which is exactly the Frobenius map of \( \mathbb{F}_{2^n} \).

**Definition 2.5** [18] Let \( f \) be an \( n \)-variable Boolean function and \( k \) be a positive integer such that \( k|n \). If \( f(\rho^k_n(x)) = f(x) \) holds for all \( x \in \mathbb{F}_2^n \), and \( k \) is the smallest integer such that this property holds, then \( f \) is called \( k \)-rotation symmetric. If \( k = 1 \), \( f \) is the usual rotation symmetric function.
In this paper, we identify $\mathbb{F}_{2^n}$ with $\mathbb{F}_2^n$ by choosing a normal basis $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$ of $\mathbb{F}_{2^n}$. Hence, the ANF of a rotation symmetric function can be transformed into the univariate expression of an idempotent function (i.e., $f(x) = f(x^2)$ for all $x \in \mathbb{F}_{2^n}$) and vice versa (see [3]). Moreover, given the normal basis, the elements $0, 1 \in \mathbb{F}_{2^n}$ can be regarded as $0, 1 \in \mathbb{F}_2^n$ respectively, since $0 = (0, \ldots, 0) = \sum_{i=0}^{n-1} 0 \times \alpha^{2^i} = 0$ and $1 = (1, \ldots, 1) = \sum_{i=0}^{n-1} 1 \times \alpha^{2^i} = \text{Tr}_1^n(\alpha) = 1$ (note that $\alpha^{2^i} \mid i = 0, \ldots, n - 1$, are linearly independent over $\mathbb{F}_2$, which implies $\text{Tr}_1^n(\alpha) \neq 0$).

Employing the Frobenius map, we define a $k$-orbit generated by $x \in \mathbb{F}_{2^n}$ as

$$O_n^{(k)}(x) = \left\{ \rho_n^0(x), \rho_n^k(x), \ldots, \rho_n^{(l-1)k}(x) \right\},$$

where $k \mid n$, and $l$ is the smallest positive integer such that $\rho_n^{lk}(x) = x$. In particular, 1-orbit of $x$ is the usual orbit, which is written as $O_n(x)$ for convenience. Every orbit can be represented by its lexicographically first element, called the representative element. The set of all representative elements in $\mathbb{F}_2^n$ is denoted by $\Omega_n$. For example, $\Omega_4 = \{(0, 0, 0, 0), (1, 0, 0, 0), (1, 1, 0, 0), (1, 0, 1, 0), (1, 1, 1, 0), (1, 1, 1, 1)\}$.

It is proved that (see e.g. [5, Appendix A.1]) the number of distinct orbits in $\mathbb{F}_2^n$, i.e., $|\Omega_n|$, is $\Psi_n = \frac{1}{n} \sum_{k|n} \phi(k) 2^{n/k}$, where $\phi(k)$ is the Euler’s phi-function.

Given $v \in \mathbb{F}_2^n$, it is clear that in the ANF of an $n$-variable $k$-rotation symmetric function, the coefficients of the monomials $x^u$, $u \in O_n^{(k)}(v)$, are all the same. For simplicity, we write $O_n^{(k)}(x^v) = \bigoplus_{u \in O_n^{(k)}(v)} x^u$.

### 3 A family of WPB functions

In this section, we propose a large class of WPB functions, which are not EA equivalent to the functions given by Carlet et al. [4]. These WPB functions are 2-rotation symmetric functions. Recall that we always assume $n$ is a power of 2.

#### 3.1 General results on the construction of WPB functions

We first present a generic construction of WPB functions.

**Theorem 3.1** For an $n$-variable Boolean function $f$, if $f(x^2) = f(x) + 1$ holds for all $x \in \mathbb{F}_{2^n} \setminus \{0, 1\}$, where $+$ is in $\mathbb{F}_2$, then $f$ is WPB.

**Proof** For $E_{n,k} = \{x \in \mathbb{F}_2^n \mid w_H(x) = k\}$, recall that $w_H(f)_k = |\{x \in E_{n,k} \mid f(x) = 1\}|$. Since for $x \in \mathbb{F}_{2^n} \setminus \{0, 1\}$, we have $f(x^2) = f(x) + 1$, i.e., $f(\rho_n^1(x)) = f(x) + 1$, then for $1 \leq k \leq n - 1$,

$$w_H(f \circ \rho_n^1)_k = \binom{n}{k} - w_H(f)_k \quad (1)$$

On the other hand, it is obvious that $\rho_n^1(E_{n,k}) = \{\rho_n^1(x) \mid x \in E_{n,k}\} = E_{n,k}$, then

$$w_H(f \circ \rho_n^1)_k = |\{x \in E_{n,k} \mid f \circ \rho_n^1(x) = 1\}|$$

$$= |\{y \in \rho_n^1(E_{n,k}) \mid f(y) = 1\}|$$
Thus, item 1 is a necessary condition of item 2. We know that the number of Boolean functions
\[
\beta
\]
where the last equation is from the fact
1
Similarly, if
2
for all
3
\[ j \in \{1, 2\} \]
Corollary 3.2 The WPB functions in Theorem 3.1 are 2-rotation symmetric.

Theorem 3.3 For a Boolean function \( f \) with \( f(0) = 0 \) and \( f(1) = 1 \), the following assertions are equivalent:
1. \( f(x^2) = f(x) + 1 \) holds for all \( x \in \mathbb{F}_{2^n} \setminus \{0, 1\} \), where \( + \) is in \( \mathbb{F}_2 \).
2. \( f(x) = \sum_{j \in \Gamma_n \setminus \{0\}} \text{Tr}^{o(j)}_1 (\beta^{ij} x^j) \), where \( \beta \) is a primitive element of \( \mathbb{F}_{2^2} \), \( ij \in \{1, 2\} \) for \( j \in \Gamma_n \setminus \{0\} \).
3. \( f(x) = \bigoplus_{v \in \Omega_n \setminus \{0, 1\}} O_n^{(2)} (\{ \rho_n^i(v) \} x^j) \), where \( iv \in \{0, 1\} \) for \( v \in \Omega_n \setminus \{0, 1\} \).

Proof We first prove that item 1 is equivalent to item 2. Note that for \( j \in \Gamma_n \setminus \{0\} \), \( o(j) \) is a divisor of \( n \), and thus even. Then, for \( g(x) = \text{Tr}^{o(j)}_1 (\beta x^j) \), we have
\[
g(x) + g(x^2) = (\beta x^j + \beta^2 x^{2j} + \cdots + \beta x^{2^{o(j)-2}j} + \beta^2 x^{2^{o(j)-1}j})
+ (\beta x^{2j} + \beta^2 x^{4j} + \cdots + \beta x^{2^{o(j)-1}j} + \beta^2 x^{2j})
= (\beta + \beta^2) \text{Tr}^{o(j)}_1 (x^j)
= \text{Tr}^{o(j)}_1 (x^j),
\]
where the last equation is from the fact \( \beta + \beta^2 = 1 \) for \( \beta \) is a primitive element of \( \mathbb{F}_{2^2} \). Similarly, if \( g(x) = \text{Tr}^{o(j)}_1 (\beta^2 x^j) \), then we can also get \( g(x) + g(x^2) = \text{Tr}^{o(j)}_1 (x^j) \). Hence, for \( f(x) = \sum_{j \in \Gamma_n \setminus \{0\}} \text{Tr}^{o(j)}_1 (\beta^{ij} x^j) \), we have that, for all \( x \in \mathbb{F}_{2^n} \setminus \{0, 1\} \),
\[
f(x) + f(x^2) = \sum_{j \in \Gamma_n \setminus \{0\}} \text{Tr}^{o(j)}_1 (x^j) = \sum_{j=1}^{2^{n-2}} x^j = 1.
\]
Thus, item 1 is a necessary condition of item 2. We know that the number of Boolean functions satisfying the condition in item 1 is \( 2^{\Psi_n - 2} \). Indeed, the truth table of \( f \) in item 1 is determined by \( f(x) \), \( x \in \Omega_n \setminus \{0, 1\} \). On the other hand, it can be checked that the number of nonzero cyclotomic classes of 2 modulo \( 2^n - 1 \) is \( \Psi_n - 2 \). In fact, if we represent the numbers \( 1, 2, \ldots, 2^n - 2 \) by \( n \)-tuples of binary digits, then it is easy to see that there is a one-to-one correspondence between the nonzero cyclotomic classes of 2 modulo \( 2^n - 1 \) and the orbits in \( \mathbb{F}_{2^n} \setminus \{0, 1\} \). For example, the cyclotomic class \( \{3, 5, 6\} \) of 2 modulo 7 is corresponding to the orbit \( \{(011), (101), (110)\} \) in \( \mathbb{F}_{2^3} \). Hence, the number of Boolean functions in item 2 is also \( 2^{\Psi_n - 2} \), which implies that item 1 is equivalent to item 2.

Now we prove that item 1 is equivalent to item 3. Recall that \( x^2 = \rho_n^1(x) \). Suppose that \( f(x) \) is defined as in item 3, then
\[ f(x) + f(x^2) = \bigoplus_{v \in \Omega_n \backslash \{0,1\}} O_n^{(2)}(x^{\rho_n^v(v)}) \oplus \bigoplus_{v \in \Omega_n \backslash \{0,1\}} O_n^{(2)}(x^{\rho_n^1(x)^{\rho_n^v(v)}}) \]

\[ = \bigoplus_{v \in \Omega_n \backslash \{0,1\}} O_n^{(2)}(x^{\rho_n^i(v)}) \oplus \bigoplus_{v \in \Omega_n \backslash \{0,1\}} O_n^{(2)}(x^{\rho_n^{i+1}(v)}) \]

\[ = \bigoplus_{\nu \in \Omega_n \backslash \{0,1\}} O_n(x^\nu) \]

\[ = 1 \oplus x_1 x_2 \cdots x_n \oplus (x_1 \oplus 1)(x_2 \oplus 1) \cdots (x_n \oplus 1). \]

It is obvious that \( 1 \oplus x_1 x_2 \cdots x_n \oplus (x_1 \oplus 1)(x_2 \oplus 1) \cdots (x_n \oplus 1) = 1 \) for all \( x \in \mathbb{F}_2^n \backslash \{0,1\} \), and thus \( f(x) \) satisfies the condition in item 1. Moreover, since \( i_v \in \{0,1\} \) for \( v \in \Omega_n \backslash \{0,1\} \), then the number of functions in item 3 is \( 2^{\Psi_n - 2} \), which is equal to the number of functions in item 1. Therefore, item 1 is equivalent to item 3. \( \square \)

**Example 3.4** Let \( \alpha \) be a primitive element of \( \mathbb{F}_{2^4} \). Then, \( \alpha^5 \) is a primitive element of \( \mathbb{F}_{2^2} \). According to Theorems 3.1 and 3.3 as well as Corollary 3.2, we have

\[ f(x) = \operatorname{Tr}_1^4(\alpha^5x) + \operatorname{Tr}_1^4(\alpha^5x^3) + \operatorname{Tr}_1^2(\alpha^5x^5) + \operatorname{Tr}_1^4(\alpha^5x^7) \]

is a 2-rotation symmetric WPB function over \( \mathbb{F}_{2^4} \). It can be checked that by decomposing \( x \in \mathbb{F}_{2^4} \) over the normal basis \( \{\alpha, \alpha^2, \alpha^4, \alpha^8\} \), the ANF of \( f(x) \) can be written as

\[ f(x) = x_1 \oplus x_2 \oplus x_1 x_4 \oplus x_2 x_3 \oplus x_1 x_3 \oplus x_1 x_2 x_4 \oplus x_2 x_3 x_4. \]

Combining Theorems 3.1, 3.3 with Corollary 3.2, we obtain a construction of WPB functions in the trace form as well as the algebraic normal form. Applying the trace form, we have the following corollary.

**Corollary 3.5** The \( n \)-variable Boolean function \( f \) of the form

\[ f(x) = \sum_{j \in \Gamma_n \backslash \{0\}} \operatorname{Tr}_1^{o(j)}(\beta^{ij} x^j) \]

is a 2-rotation symmetric WPB function with \( \deg(f) = n - 1 \), where \( \beta \) is a primitive element of \( \mathbb{F}_{2^2} \), \( i, j \in \{1, 2\} \) for \( j \in \Gamma_n \backslash \{0\} \).

**Proof** From Theorems 3.1, 3.3, and Corollary 3.2, we only need to show that \( \deg(f) = n - 1 \). In fact, since the coefficients \( \beta^{ij} \neq 0 \) for all \( j \in \Gamma_n \backslash \{0\} \), then

\[ \deg(f) = \max\{\operatorname{wt}(j) \mid j \in \Gamma_n \backslash \{0\}\} = \operatorname{wt}(2^n - 2) = n - 1. \]

\( \square \)

**Remark 3.6** From the proof of Theorem 3.3, we know that the number of WPB functions constructed in Corollary 3.5 is \( 2^{\Psi_n - 2} \).

**Remark 3.7** In [4, Proposition 3], Carlet et al. recursively built a class of WPB functions of \( n = 2^k \) variables, which have algebraic degree \( n/2 \). Since the algebraic degree of the functions in (3) is \( n - 1 \), we know that the WPB functions in (3) are not EA equivalent to that in [4, Proposition 3], and thus we obtain a new construction of WPB functions.
From the cryptanalysis viewpoint, the algebraic degree of a Boolean function should be high, but for Boolean functions applied to the filter permutator model (e.g. cipher FLIP), the homomorphic-friendly design requires to reduce the multiplicative depth of the decryption circuit. That is to say, a lower algebraic degree is preferred. There exists a trade-off between the security and the homomorphic performance.

### 3.2 Analysis of the weightwise nonlinearity profile of WPB functions

In this subsection, we mainly discuss the weightwise nonlinearity profile of WPB functions. For an $n$-variable Boolean function $f$, one can easily prove that $f$ is equal to some linear function when restricted to $E_{n,1} = \{ x \in \mathbb{F}_2^n \mid w_H(x) = 1 \}$. In particular, we get the following result.

**Proposition 3.8** For any WPB function $f$, we have $\text{NL}_1(f) = 0$.

Krawtchouk polynomial (see [15]) of degree $k$ is defined by $K_k(i, n) = \sum_{j=0}^{k} (-1)^j \binom{i}{j} \binom{n-j}{k-j}$. It is known that $\sum_{x \in E_{n,k}} (-1)^{a \cdot x} = K_k(w_H(a), n)$. We apply Krawtchouk polynomial to explore the weightwise nonlinearity of WPB functions.

**Theorem 3.9** For a WPB function $f$, the $k$-weight nonlinearity of $f$ can be calculated by

$$\text{NL}_k(f) = \frac{1}{2} \binom{n}{k} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \left| \sum_{x \in E_{n,k}} (-1)^{f(x) \oplus a \cdot x} \right|.$$

where $S(f) = \{ x \in \mathbb{F}_2^n \mid f(x) = 1 \}$.

**Proof** According to Proposition 2.3, we have

$$\text{NL}_k(f) = \frac{1}{2} \binom{n}{k} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \left| \sum_{x \in E_{n,k}} (-1)^{f(x) \oplus a \cdot x} \right|. \quad (4)$$

If $w_H(a) > n/2$, then define $\overline{a} = a \oplus 1$, where $a \oplus 1 = (a_1 \oplus 1, \ldots, a_n \oplus 1)$, and thus $0 \leq w_H(\overline{a}) < n/2$. Since

$$\left| \sum_{x \in E_{n,k}} (-1)^{f(x) \oplus \pi \cdot x} \right| = \left| \sum_{x \in E_{n,k}} (-1)^{f(x) \oplus (a \oplus 1) \cdot x} \right|$$

$$= \left| \sum_{x \in E_{n,k}} (-1)^{f(x) \oplus a \cdot x \oplus w_H(x)} \right|$$

$$= (-1)^k \left| \sum_{x \in E_{n,k}} (-1)^{f(x) \oplus a \cdot x} \right| = \left| \sum_{x \in E_{n,k}} (-1)^{f(x) \oplus a \cdot x} \right|,$$

and noting that $\left| \sum_{x \in E_{n,k}} (-1)^{f(x)} \right| = 0$ because $f$ is balanced on $E_{n,k}$, then we have

$$\text{NL}_k(f) = \frac{1}{2} \binom{n}{k} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \left| \sum_{1 \leq w_H(a) \leq n/2} (-1)^{f(x) \oplus a \cdot x} \right|. \quad (5)$$
Moreover, let \( S(f)^c = \mathbb{F}_2^n \setminus S(f) \), then we have
\[
\sum_{x \in E_{n,k}} (-1)^{f(x) \oplus a \cdot x} = \sum_{x \in E_{n,k} \cap S(f)} (-1)^{f(x) \oplus a \cdot x} + \sum_{x \in E_{n,k} \cap S(f)^c} (-1)^{f(x) \oplus a \cdot x} \\
= \sum_{x \in E_{n,k} \cap S(f)} (-1)^{a \cdot x} + \sum_{x \in E_{n,k} \cap S(f)^c} (-1)^{a \cdot x} \\
= \sum_{x \in E_{n,k} \cap S(f)} (-1)^{a \cdot x} - 2 \sum_{x \in E_{n,k} \cap S(f)^c} (-1)^{a \cdot x} \\
= K_k(w_H(a), n) - \sum_{x \in E_{n,k} \cap S(f)} (-1)^{a \cdot x}. \tag{6}
\]

Combining (5) with (6), we obtain the desired result. \( \Box \)

Let \( \Omega_{n,k} \) denote the set of all the representative elements with Hamming weight \( k \) in \( \mathbb{F}_2^n \). Then, we have the following result for WPB functions in (3).

**Theorem 3.10** For a WPB function \( f \) in (3), we have
\[
\text{NL}_k(f) = \frac{1}{2} \binom{n}{k} - \frac{1}{2} \max_{a \in \mathbb{F}_2^d : a \not\in \Omega_{n,d}} \left| K_k(w_H(a), n) - 2 \sum_{x \in \bigcup_{v \in \Omega_{n,k}} O_n(2)\left(\rho^n_i(v)\right)} (-1)^{a \cdot x} \right|, \tag{7}
\]
where \( 2 \leq k \leq n - 1 \), and for every \( v \in \Omega_{n,k}, i_v \in \{0, 1\} \) satisfies \( f(\rho^n_i(v)) = 1 \).

**Proof** From \( f(x^2) = f(x) + 1 \), we know that \( f(\rho^n_1(x)) = f(x) \). Since \( f(\rho^n_{i_v}(v)) = 1 \) for all \( v \in \Omega_{n,k} \), then we have
\[
E_{n,k} \cap S(f) = \bigcup_{v \in \Omega_{n,k}} O_n(2)\left(\rho^n_i(v)\right), \tag{8}
\]
where \( S(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 1\} \). It is obvious that if \( x \in E_{n,k} \), then \( x^2 = \rho^n_1(x) \in E_{n,k} \). Note that \( \text{Tr}^n_1(x) = \text{Tr}^n_1(x^2) \) for \( x \in \mathbb{F}_2^n \). Then, for \( a \in \mathbb{F}_2^n \), we have
\[
\sum_{x \in E_{n,k}} (-1)^{f(x) + \text{Tr}^n_1(ax)} = \sum_{x^2 \in E_{n,k}} (-1)^{f(x^2) + \text{Tr}^n_1(ax^2)} \\
= \sum_{x \in E_{n,k}} (-1)^{f(x) + 1 + \text{Tr}^n_1(a^{2^n-1}x)} \\
= - \sum_{x \in E_{n,k}} (-1)^{f(x) + \text{Tr}^n_1(a^{2^n-1}x)},
\]
and thus \( |\sum_{x \in E_{n,k}} (-1)^{f(x) \oplus \rho^n_{2^n-1}(a) \cdot x}| = |\sum_{x \in E_{n,k}} (-1)^{f(x) \oplus a \cdot x}| \). Due to Eq. (4) and Theorem 3.9, we obtain the desired result. \( \Box \)

We now focus on general lower bounds on the \( k \)-weight nonlinearity of WPB functions in (3). Let \( \text{NL}^{(n)}_k \) denote the lower bound on \( k \)-weight nonlinearity for all WPB functions over \( \mathbb{F}_{2^n} \) in (3), i.e., for any WPB function \( f \) over \( \mathbb{F}_{2^n} \) in (3), \( \text{NL}_k(f) \geq \text{NL}^{(n)}_k \). Then, we have the following result.

**Theorem 3.11** For \( 1 \leq k \leq n/2 \), \( \text{NL}^{(n)}_{n-k} = \text{NL}^{(n)}_k \). \( \Box \)
Proof It is clear that \( E_{n, n-k} = \{ x \oplus 1 \mid x \in E_{n,k} \} \), where \( x \oplus 1 = (x_1 \oplus 1, \ldots, x_n \oplus 1) \). Then, for any WPB function \( f \) in (3), there exists a WPB function \( g \) in (3) such that \( f(x) = g(x \oplus 1) \) for any \( x \in E_{n,k} \). Hence, \( \text{NL}_k(f) = \text{NL}_{n-k}(g) \geq \text{NL}_{n-k}^{(n)} \), and thus \( \text{NL}_k^{(n)} \geq \text{NL}_{n-k}^{(n)} \).

Conversely, there exists another WPB function \( h \) in (3) such that \( f(x) = h(x \oplus 1) \) for any \( x \in E_{n,n-k} \). Hence, \( \text{NL}_{n-k}(f) = \text{NL}_k(h) \geq \text{NL}_k^{(n)} \), and thus \( \text{NL}_{n-k}^{(n)} \geq \text{NL}_k^{(n)} \). Therefore, we obtain \( \text{NL}_{n-k}^{(n)} = \text{NL}_k^{(n)} \).

\( \square \)

Remark 3.12 Because of Proposition 3.8 and Theorem 3.11, we only need to consider \( \text{NL}_k^{(n)} \), where \( 2 \leq k \leq n/2 \).

Example 3.13 In Table 1, we calculate the weightwise nonlinearity profile for all \( f \) in (3) with \( n = 8 \) variables by MAGMA. Due to Proposition 3.8 and the proof of Theorem 3.11, we only need to consider \( \text{NL}_k(f) \) for \( k = 2, 3, 4 \). It is shown that for the best case, the \( k \)-weight nonlinearity of \( f \) is near the upper bound in Proposition 2.4. In particular, if \( f \) satisfies

\[
f(0, 1, 1, 1, 0, 0, 0, 0) \neq f(1, 1, 0, 1, 0, 0, 0, 0),
\]

then \( \text{NL}_3(f) \geq 8 \) (by MAGMA). Note that \((0, 1, 1, 1, 0, 0, 0, 0)\) and \((1, 1, 0, 1, 0, 0, 0, 0)\) are in different orbits.

| \( k \)-Weight nonlinearity of \( f \) | \( (\ell_k^{n})/2 - \sqrt{(\ell_k^{n})}/2 \) |
|--------------------------------------|---------------------------------------|
| \( \text{NL}_2(f) \in \{6, 9\} \)     | 11                                    |
| \( \text{NL}_3(f) \in \{0, 8, 14, 16, 18, 20, 21, 22\} \) | 24                                    |
| \( \text{NL}_4(f) \in \{19, 22, 23, 24, 25, 26, 27\} \) | 30                                    |

Theorem 3.14 For any \( n = 2^l \geq 8 \), we have

\[
\text{NL}_2^{(n)} \geq \begin{cases} 5, & \text{if } 1 \leq i \leq l - 3, \\ 6, & \text{if } i = l - 2, \\ 19, & \text{if } i = l - 1. \end{cases}
\]

Proof We first prove that for any \( n \geq 8 \), \( \text{NL}_2^{(n)} \geq 5 \). For a Boolean function \( f \), it is clear that \( \text{NL}_E(f) \geq \text{NL}_S(f) \) if \( S \subseteq E \). Let

\[
S = \{(1, 1, 0, 0, 0, 0, 0, 0, \ldots, 0), (0, 1, 1, 0, 0, 0, 0, 0, \ldots, 0), \\
(0, 1, 0, 0, 0, 0, 0, 0, \ldots, 0), (0, 0, 1, 1, 0, 0, 0, 0, \ldots, 0), \\
(0, 0, 0, 1, 1, 0, 0, 0, \ldots, 0), (0, 0, 0, 0, 0, 0, 0, 0, 0, \ldots, 0), \\
(0, 0, 0, 1, 0, 0, 0, 0, 0, \ldots, 0), (0, 1, 0, 1, 0, 0, 0, 0, \ldots, 0), \\
(0, 0, 1, 0, 1, 0, 0, 0, 0, \ldots, 0), (0, 0, 0, 1, 0, 0, 0, 0, \ldots, 0), \\
(0, 0, 1, 0, 0, 1, 0, 0, 0, \ldots, 0), (0, 0, 0, 1, 0, 0, 0, 0, \ldots, 0), \\
(0, 0, 1, 0, 0, 0, 1, 0, 0, \ldots, 0), (0, 0, 0, 0, 1, 0, 0, 0, \ldots, 0), \\
(0, 0, 1, 0, 0, 0, 0, 1, 0, \ldots, 0), (0, 0, 0, 0, 0, 1, 0, 0, \ldots, 0), \\
(0, 0, 0, 0, 1, 0, 0, 1, 0, \ldots, 0), (0, 0, 0, 0, 0, 0, 1, 0, \ldots, 0). \}
\]
Proof

We only need to prove that for 3

It is obvious that $S$ is a subset of $E_{n,2}$ for any $n \geq 8$, and there exist 4 subsets of distinct orbits respectively in $S$. Since for any $x \in S$, $x = (x_1, \ldots, x_8, 0, \ldots, 0)$, then we only need to consider $a \cdot x$ with $a = (a_1, \ldots, a_8, 0, \ldots, 0)$ as linear functions on $S$. By a tedious but easy computation, we find that for any $f$ in (3), $NL_S(f) \geq 5$, and thus $NL_2(f) \geq 5$. Hence, $NL_2(\rho_{(n)}) \geq 5$ for $n \geq 8$. In particular, we have $NL_2(\rho_{(8)}) \geq 6$ according to Table 1.

For any $n = 2^l \geq 8$ and any $2 \leq i \leq l - 1$, let

$$R = \{ (y, y) \mid y \in \mathbb{F}_2^{n/2}, w_H(y) = 2^{i-1} \}. $$

Clearly, for any $x = (y, y) \in R$, the orbit generated by $x$ satisfies

$$O_n(x) = \left\{ (z, z) \mid z \in O_{n/2}(y) \right\}. $$

Then, for any WPB function $f$ over $\mathbb{F}_{2^n}$ in (3), there must exist a WPB function $g$ over $\mathbb{F}_{2^{n/2}}$ in (3) such that $f(x) = g(y)$, where $x = (y, y) \in R$. Since $R \subseteq E_{n,2^l}$ and $E_{n/2,2^{l-1}} = \{ y \in \mathbb{F}_2^{n/2} \mid w_H(y) = 2^{i-1} \}$, then $NL_2(f) \geq NL_R(f) = NL_{2^{l-1}}(g)$, which leads to

$$NL_2(\rho_{(n/2^{l-1})}) \geq \cdots \geq \begin{cases} NL_2(\rho_{(n/2^{l-1})}) \geq 5, & \text{if } 1 \leq i \leq l - 3, \\ NL_2(\rho_{(8)}) \geq 6, & \text{if } i = l - 2, \\ NL_2(\rho_{(8)}) \geq 19, & \text{if } i = l - 1, \\ \end{cases}$$

where $NL_2(\rho_{(8)}) \geq 19$ is according to Table 1. \hfill \Box

4 A primary construction of WPB functions with high weightwise nonlinearity profile

In this section, we propose Construction-1 as a subclass of WPB functions in (3). We prove that these WPB functions have high weightwise nonlinearity profile. From Theorem 3.3, we know that to obtain a WPB function $f$ in (3), one only needs to define the values of $f$ on all the representative elements of the orbits in $\mathbb{F}_2^n$. So, in Construction-1 below, we only define $f$ on the representative elements of the orbits in $\mathbb{F}_2^n$. Recall that $\Omega_{n,k}$ denotes the set of all the representative elements with Hamming weight $k$ in $\mathbb{F}_2^n$. By the following lemma, we give more explanations on Construction-1.

Lemma 4.1 Construction-1 outputs an $n$-variable WPB function.

Proof

We only need to prove that for $3 \leq k \leq n/2$, $\bigcup_{y_1 \in Y_k} R_{y_1}$ (for $k$ odd) and $\bigcup_{y_1 \in Y_k} (T_{y_1} \cup S_{y_1})$ (for $k$ even) consist of distinct orbits respectively in $\mathbb{F}_2^n$. Thus, by Construction-1, we can define a WPB function satisfying $f(x) = f(x^2) + 1$ for $x \in \mathbb{F}_{2^n} \setminus \{0,1\}$.

For $\bigcup_{y_1 \in Y_k} R_{y_1}$, suppose that there exists some $j \geq 1$ such that $x_1 = \rho_{n}^j(x_2)$, where $x_1, x_2 \in \bigcup_{y_1 \in Y_k} R_{y_1}$. Then, since the first coordinate of $x_1$ is 1, then it must be the case that $\rho_{n}^j(x_2) = (y''_1, \mathbf{0}_1, y_2, 1, y''_1)$ or $\rho_{n}^j(x_2) = (y''_1, 1, y_1, \mathbf{0}_1, y''_2)$, where $x_2 = (1, y_1, \mathbf{0}_1, y_2)$, $(y'_1, y''_1) = y_1 \in \mathbb{F}_2^{n/4-1}$, $(y'_2, y''_2) = y_2 \in \mathbb{F}_2^{n/2}$, $w_H(y_1) = i - 2$, $w_H(y_2) = i$. \hfill \circ
1. If \( n = 8 \), then output any function in (3) with constraints
\[
f(0, 1, 1, 1, 0, 0, 0, 0) \neq f(1, 1, 1, 0, 0, 0, 0, 0), \quad f(0, 0, 1, 1, 1, 1, 1, 1) \neq f(0, 0, 1, 1, 0, 0, 1, 1).
\]
2. If \( n \geq 16 \), let \( f(0) = 0, f(1) = 1 \). Define \( Y_k = \{ y \in F_2^{n/4} \mid w_H(y) = \lceil k/2 \rceil - 2 \} \) for \( 3 \leq k \leq n/2 \), then

2.1. For \( x \in \Omega_{n,2} \), \( f(x) \) is chosen randomly in \( F_2 \).

2.2. If \( k = 2i - 1, 2 \leq i \leq n/4 \). For \( y_1 \in Y_k \), let the zero vector \( \mathbf{0}_1 \in F_2^{n/4} \),
\[
R_{y_1} = \{(1, y_1, 0, y_2) \mid y_2 \in F_2^{n/2}, w_H(y_2) = i \},
\]
and for \( x = (1, y_1, 0, y_2) \in R_{y_1} \), define \( f(x) = g(y_2) \) and \( f(\overline{x}) = h(\overline{y_2}) \), where \( g, h \) are \( n/2 \)-variable functions in Construction-1, and \( \overline{x} \) denotes the complement of \( x \), i.e., \( \overline{x} = x \oplus 1, 1 = (1, \ldots, 1) \).

For \( x \in (\Omega_{n,k} \cup \Omega_{n,n-k}^{-}) \setminus \bigcup_{y_1 \in Y_k} (R_{y_1} \cup \overline{R_{y_1}}) \), \( f(x) \) is chosen randomly in \( F_2 \), where \( \overline{A} = \{ x \mid x \in A \} \).

2.3. If \( k = 2i, 2 \leq i \leq n/4 \). For \( y_1 \in Y_k \), let the zero vectors \( \mathbf{0}_1 \in F_2^{n/4} \), \( \mathbf{0}_2 \in F_2^{n/4-1} \),
\[
T_{y_1} = \{(1, y_1, 0, y_2) \mid y_2 \in F_2^{n/2}, w_H(y_2) = i + 1 \},
\]
\[
S_{y_1} = \{(1, y_1, 0, 2, y_2) \mid y_2 \in F_2^{n/2}, w_H(y_2) = i, y_2 \neq (y, \mathbf{0}_2, 1, 1) \text{ for all } y \in Y_k \},
\]
and for \( x_1 = (1, y_1, \mathbf{0}_1, y_2) \in T_{y_1} \), \( x_2 = (1, y_1, \mathbf{0}_1, 2, z_2) \in S_{y_1} \), define \( f(x_1) = g_2(y_2) \), \( f(x_2) = y_2(z_2) \), and for \( k < n/2 \), define \( f(\overline{x_1}) = h_1(\overline{y_2}) \), \( f(\overline{x_2}) = \overline{y_2}(\overline{z_2}) \), where \( g_2, h_1, h_2 \) are \( n/2 \)-variable functions in Construction-1.

For \( x \in (\Omega_{n,k} \cup \Omega_{n,n-k}^{-}) \setminus \bigcup_{y \in Y_k} (T_{y_1} \cup S_{y_1} \cup \overline{T_{y_1}} \cup \overline{S_{y_1}}) \), \( f(x) \) is chosen randomly in \( F_2 \).

2.4. Define \( f(x) = f(x^2) + 1 \) for \( x \in F_2^n \setminus \{0, 1, \Omega_n\} \).

- Suppose \( \rho_n^j(x_2) = (y''_2, \mathbf{0}_2, y_2, 1, y''_1) = (1, z_1, \mathbf{0}_1, z_2) = x_1 \in R_{z_1} \). Since \( w_H(y''_2) \leq i - 2 \), and the first coordinate of \( y''_1 \) is 1, then \( w_H(z_1) \leq i - 3 \), which contradicts with \( w_H(z_1) = i - 2 \).
- Suppose \( \rho_n^j(x_2) = (y''_2, 1, y_1, y''_1) = (1, z_1, \mathbf{0}_1, z_2) = x_1 \in R_{z_1} \). Since \( w_H(1, y_1) = i - 1 \), and the first coordinate of \( y''_2 \) is 1, then \( w_H(z_1) \geq i - 1 \), which contradicts with \( w_H(z_1) = i - 2 \).

Therefore, all the elements in \( \bigcup_{y_1 \in Y_k} R_{y_1} \) belong to different orbits in \( F_2^n \).

For \( \bigcup_{y_1 \in Y_k} (T_{y_1} \cup S_{y_1}) \), since we can prove similarly that all the elements in \( \bigcup_{y_1 \in Y_k} T_{y_1} \) belong to different orbits in \( F_2^n \), then we only consider the following two cases.

1. Suppose that there exists some \( j \geq 1 \) such that \( x_1 = \rho_n^j(x_2) \), where \( x_1, x_2 \in \bigcup_{y_1 \in Y_k} S_{y_1} \). Since the first coordinate of \( x_1 \) is 1, then it must be the case that \( \rho_n^j(x_2) = (1, y_2, 1, y_1, \mathbf{0}_2) \), \( \rho_n^j(x_2) = (y''_2, \mathbf{0}_2, 1, y_2, 1, y''_1) \), or \( \rho_n^j(x_2) = (y''_2, 1, y_1, \mathbf{0}_2, 1, y''_1) \), where \( x_2 = (1, y_1, \mathbf{0}_2, 1, y_2, y''_1, y''_2) = y_1 \in F_2^{n/4-1}, (y''_2, y''_2) = y_2 \in F_2^{n/2}, w_H(y_1) = i - 2, w_H(y_2) = i \).

- Suppose \( \rho_n^j(x_2) = (1, y_2, 1, y_1, \mathbf{0}_2) = (1, z_1, \mathbf{0}_2, 1, z_2) = x_1 \in S_{z_1} \). Let \( y_2 = (b_1, b_2) \in F_2^{n/2-1} \times F_2 \). Since \( w_H(1, b_1) = w_H(1, z_1, \mathbf{0}_2, 1) = i \) and \( w_H(y_2) = i \), then \( b_2 = 1 \), and thus \( y_2 = (z_1, \mathbf{0}_2, 1, 1) \), which contradicts with the condition \( y_2 \neq (y, \mathbf{0}_2, 1, 1) \) for \( y \in Y_k \).
- Suppose \( \rho_n^j(x_2) = (y''_2, \mathbf{0}_2, 1, y_2, 1, y''_1) = (1, z_1, \mathbf{0}_2, 1, z_2) = x_1 \in S_{z_1} \). Since \( w_H(y''_2) \leq i - 2 \), and the first coordinate of \( y''_1 \) is 1, then \( w_H(z_1) \leq i - 3 \), which contradicts with \( w_H(z_1) = i - 2 \).
Lemma 4.2

Suppose that $\rho_n^j(x_2) = (y''_2, 1, y_1, 0_2, 1, y'_2) = (1, z_1, 0_2, 1, z_2) = x_1 \in S_{z_1}$. Since $w_H(1, y_1) = i - 1$, and the first coordinate of $y''_2$ is 1, then $w_H(z_1) \geq i - 1$, which contradicts with $w_H(z_1) = i - 2$.

Therefore, all the elements in $\bigcup_{y_1 \in T_{y_1}} S_{y_1}$ belong to different orbits in $\mathbb{F}_2^n$.

2. Suppose that there exists some $j \geq 1$ such that $x_1 = \rho_n^j(x_2)$, where $x_1 \in \bigcup_{y_1 \in T_{y_1}} S_{y_1}$.

Since the first coordinate of $x_1$ is 1, then it must be the case that $\rho_n^j(x_2) = (1, y_2, 1, y_1, 0_2)$, $\rho_n^j(x_2) = (y''_2, 0_2, 1, y_2, 1, y'_1)$, or $\rho_n^j(x_2) = (y''_2, 1, y_1, 0_2, 1, y'_2)$, where $x_2 = (1, y_1, 0_2, 1, y_2, (y'_1, y''_1)) = y_1 \in \mathbb{F}_2^{n/4-1}$, $(y''_2, y'_2) = y_2 \in \mathbb{F}_2^{n/2}$, $w_H(y_1) = i - 2$, $w_H(y_2) = i$.

• Suppose $\rho_n^j(x_2) = (1, y_2, 1, y_1, 0_2) = (1, z_1, 0_1, 0_2) = x_1 \in T_{z_1}$. Let $y_2 = (b_1, b_2) \in \mathbb{F}_2^{n/2-1} \times \mathbb{F}_2$, then $(1, b_1) = (1, z_1, 0_1)$. Since $w_H(y_2) = i$, then $w_H(1, b_1) \geq i$, which contradicts with $w_H(1, z_1, 0_1) = i - 1$.

• Suppose $\rho_n^j(x_2) = (y''_2, 0_2, 1, y_2, 1, y'_1) = (1, z_1, 0_1, z_2) = x_1 \in T_{z_1}$. Since $w_H(y''_2) \leq i - 2$, and the first coordinate of $y''_2$ is 1, then $w_H(z_1) \leq i - 3$, which contradicts with $w_H(z_1) = i - 2$.

• Suppose $\rho_n^j(x_2) = (y''_2, 1, y_1, 0_2, 1, y'_2) = (1, z_1, 0_1, z_2) = x_1 \in T_{z_1}$. Since $w_H(1, y_1) = i - 1$, and the first coordinate of $y''_2$ is 1, then $w_H(z_1) \geq i - 1$, which contradicts with $w_H(z_1) = i - 2$.

Therefore, $\bigcup_{y_1 \in T_{y_1}} T_{y_1}$ and $\bigcup_{y_1 \in T_{y_1}} S_{y_1}$ consist of different orbits in $\mathbb{F}_2^n$. In conclusion, for any $3 \leq k \leq n/2$, $\bigcup_{y_1 \in T_{y_1}} R_{y_1}$ and $\bigcup_{y_1 \in T_{y_1}} (T_{y_1} \cup S_{y_1})$ consist of distinct orbits in $\mathbb{F}_2^n$.

We now discuss about the lower bounds on weightwise nonlinearity profile of WPB functions in Construction-1. Let $nl_k^{(n)}$ denote the lower bound on $k$-weight nonlinearity for all $n$-variable WPB functions in Construction-1, i.e., for any $n$-variable WPB function $f$ in Construction-1, $NL_k(f) \geq nl_k^{(n)}$. Similar to the proof of Theorem 3.11, we can obtain $nl_k^{(n)} = nl_{n-k}^{(n)}$. Hence, in the following, one only needs to consider $nl_k^{(n)}$ for $2 \leq k \leq n/2$.

Before present the lower bound in Theorem 4.4, we first see the following lemmas.

Lemma 4.2 For a set $E \subseteq \mathbb{F}_2^n$, define $\rho_n^j(E) = \{\rho_n^j(x) \mid x \in E\}$. If an $n$-variable Boolean function $f$ satisfies $f(x) = f(x^2) + 1$ for all $x \in E$, then $NL_{\rho_n^j(E)}(f) = NL_E(f)$.

Proof Since $f(x) = f(x^2) + 1$ for all $x \in E$, then for any $a \in \mathbb{F}_2^n$,

$$\sum_{x \in \rho_n^j(E)} (-1)^f(x) + \text{Tr}_1^n(ax) = \sum_{x \in E} (-1)^f(x) + \text{Tr}_1^n(ax^2) = -\sum_{x \in E} (-1)^f(x) + \text{Tr}_1^n(ax^{a^n-1})$$

Hence, we have

$$NL_{\rho_n^j(E)}(f) = \frac{1}{2} |\rho_n^j(E)| - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \left| \sum_{x \in \rho_n^j(E)} (-1)^f(x) + \text{Tr}_1^n(ax) \right|$$

$$= \frac{1}{2} |E| - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \left| \sum_{x \in E} (-1)^f(x) + \text{Tr}_1^n(ax) \right| = NL_E(f).$$

The following lemma is straightforward, and its proof is omitted.

Lemma 4.3 Let $x = (x_1, x_2) \in \mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2}$, where $n = 2^k$ for some positive integer $k$. If $x_1 \neq x_2$, then the orbit generated by $x$ has length $n$. 

 Springer
Theorem 4.4 For \( n \geq 8 \) and \( 2 \leq i \leq n/4 \), we have the following lower bound on weighwise nonlinearity profile recursively,

\[
\begin{align*}
n_{i}^{(n)} & \geq 5, \\
n_{2i}^{(n)} & \geq n \left( \frac{n/4 - 1}{i - 2} \right) n_{i}^{(n/2)}, \\
n_{2i}^{(n)} & \geq \frac{n}{2} \left( \frac{n/4 - 1}{i - 2} \right) \left( 2n_{i}^{(n/2)} - 2 \left( \frac{n/4 - 1}{i - 2} \right) - 1 \right) + n \left( \frac{n/4 - 1}{i - 2} \right) n_{i+1}^{(n/2)}.
\end{align*}
\]

Proof For any \( n \)-variable WPB function \( f \) in Construction-1, we first consider the case

\( k = 2i - 1 \) for some \( 2 \leq i \leq n/4 \). Since for any \( y_{1} \in Y_{k} \), \( f(x) = g(y_{2}) \) for all \( x = (1, y_{1}, 0_{1}, y_{2}) \in R_{y_{1}} \). So, we have

\[
NL_{R_{y_{1}}}(f) = NL_{i}(g) \geq n_{i}^{(n/2)}.
\]

(10)

Since \( f(x) = f(x^{2}) + 1 \) for all \( x \in \rho_{n}^{j}(E) \), where \( j = 0, 1, \ldots, n - 1 \), then applying Lemma 4.2 recursively, we have \( NL_{\rho_{n}^{j}(R_{y_{1}})}(f) = NL_{R_{y_{1}}}(f) \) for any \( 0 \leq j \leq n - 1 \). Because \( k \) is odd, then from Lemma 4.3, we know that the orbit generated by \( x \) has length \( n \). Hence, \( \left| \bigcup_{j=0}^{n-1} \rho_{n}^{j}(R_{y_{1}}) \right| = n \cdot |R_{y_{1}}| \), and thus (10) leads to

\[
NL_{\bigcup_{j=0}^{n-1} \rho_{n}^{j}(R_{y_{1}})}(f) \geq n \cdot NL_{\rho_{n}^{j}(R_{y_{1}})}(f) = n \cdot NL_{R_{y_{1}}}(f) \geq n \cdot n_{i}^{(n/2)}.
\]

(11)

Let \( Y = \bigcup_{y_{1} \in Y_{k}} \bigcup_{j=0}^{n-1} \rho_{n}^{j}(R_{y_{1}}) \), then according to (11), we obtain

\[
NL_{Y}(f) \geq |Y_{k}| \cdot NL_{\bigcup_{j=0}^{n-1} \rho_{n}^{j}(R_{y_{1}})}(f) \geq n \left( \frac{n/4 - 1}{i - 2} \right) n_{i}^{(n/2)}.
\]

Note that \( Y \subseteq E_{n,k} \). Then, \( NL_{k}(f) \geq NL_{Y}(f) \), and thus \( n_{i}^{(n)} \geq n \left( \frac{n/4 - 1}{i - 2} \right) n_{i}^{(n/2)} \).

Let \( k = 2i \) with \( 2 \leq i \leq n/4 \). Since for any \( y_{1} \in Y_{k} \), \( f(x_{1}) = g_{1}(y_{2}) \) and \( f(x_{2}) = g_{2}(z_{2}) \) for all \( x_{1} = (1, y_{1}, 0_{1}, y_{2}) \in T_{y_{1}} \) and \( x_{2} = (1, y_{1}, 0_{1}, 1, z_{2}) \in S_{y_{1}} \). So, we have

\[
\begin{align*}
NL_{T_{y_{1}}}(f) & = NL_{i+1}(g_{1}) \geq n_{i}^{(n/2)}, \\
NL_{S_{y_{1}}}(f) & = NL_{i}(g_{2}) - |Y_{k}| \geq n_{i}^{(n/2)} - \left( \frac{n/4 - 1}{i - 2} \right).
\end{align*}
\]

(12)

(13)

where (13) is because \( z_{2} \neq (y, 0_{2}, 1, 1) \) for all \( y \in Y_{k} \). From Lemma 4.3, we know that for any \( x = (1, y_{1}, 0_{1}, y_{2}) \in T_{y_{1}} \), the orbit generated by \( x \) has length \( n \). Also, for any \( x = (1, y_{1}, 0_{2}, 1, z_{2}) \in S_{y_{1}} \), the orbit generated by \( x \) has length \( n/2 \) if \( z_{2} = (1, y_{1}, 0_{2}, 1) \), and \( n \) otherwise. Then, \( \left| \bigcup_{j=0}^{n-1} \rho_{n}^{j}(T_{y_{1}}) \right| = n \cdot |T_{y_{1}}| \), \( \left| \bigcup_{j=0}^{n/2-1} \rho_{n}^{j}(S_{y_{1}}) \right| = n/2 \cdot |S_{y_{1}}| \), and \( \left| \bigcup_{j=n/2}^{n-1} \rho_{n}^{j}(S_{y_{1}}) \setminus \{(1, y_{1}, 0_{2}, 1, 1, y_{1}, 0_{2}, 1)\} \right| = n/2 \cdot |S_{y_{1}}| - 1 \). Define

\[
\begin{align*}
T & = \bigcup_{y_{1} \in Y_{k}} \bigcup_{j=0}^{n-1} \rho_{n}^{j}(T_{y_{1}}), \\
S & = \bigcup_{y_{1} \in Y_{k}} \bigcup_{j=0}^{n/2-1} \rho_{n}^{j}(S_{y_{1}}), \\
S_{2} & = \bigcup_{y_{1} \in Y_{k}} \bigcup_{j=n/2}^{n-1} \rho_{n}^{j}(S_{y_{1}} \setminus \{(1, y_{1}, 0_{2}, 1, 1, y_{1}, 0_{2}, 1)\})).
\end{align*}
\]
Table 2  Lower bound on weightwise nonlinearity profile of \( f \) with \( n = 16 \) variables

| \( k \)-Weight nonlinearity of \( f \) | Upper bound |
|-----------------------------------|-------------|
| \( \text{NL}_2(f) \geq 5 \)       | 54          |
| \( \text{NL}_3(f) \geq 144 \)     | 268         |
| \( \text{NL}_4(f) \geq 472 \)     | 888         |
| \( \text{NL}_5(f) \geq 1056 \)    | 2150        |
| \( \text{NL}_6(f) \geq 2184 \)    | 3959        |
| \( \text{NL}_7(f) \geq 1296 \)    | 5666        |
| \( \text{NL}_8(f) \geq 2184 \)    | 6378        |

Then, we have

\[
\text{NL}_{T \cup S_1 \cup S_2}(f) \geq \text{NL}_T(f) + \text{NL}_{S_1}(f) + \text{NL}_{S_2}(f)
\]

\[
= n \cdot |Y_k| \cdot \text{NL}_{\rho_i^k(T_{y_1})}(f) + \frac{n}{2} \cdot |Y_k| \cdot \text{NL}_{\rho_i^k(S_{y_1})}(f)
\]

\[
+ \frac{n}{2} \cdot |Y_k| \cdot \left( \text{NL}_{\rho_i^k(S_{y_1})}(f) - 1 \right)
\]

\[
= n \cdot |Y_k| \cdot \text{NL}_{T_{y_1}}(f) + \frac{n}{2} \cdot |Y_k| \cdot \text{NL}_{S_{y_1}}(f) + \frac{n}{2} \cdot |Y_k| \cdot \left( \text{NL}_{S_{y_1}}(f) - 1 \right)
\]

(14)

\[
\geq n \binom{n/4 - 1}{i - 2} \binom{n/2}{i + 1} + \frac{n}{2} \binom{n/4 - 1}{i - 2} \left( \binom{n/2}{i} - \binom{n/4 - 1}{i - 2} \right)
\]

\[
+ \frac{n}{2} \binom{n/4 - 1}{i - 2} \left( \binom{n/2}{i} - \binom{n/4 - 1}{i - 2} - 1 \right)
\]

\[
= n \binom{n/4 - 1}{i - 2} \binom{n/2}{i + 1} + \frac{n}{2} \binom{n/4 - 1}{i - 2} \left( 2\binom{n/2}{i} - 2\binom{n/4 - 1}{i - 2} - 1 \right).
\]

(15)

where (14) is due to Lemma 4.2, and (15) is from (12) and (13). Note that \( T \cup S_1 \cup S_2 \subseteq E_{n,k} \). Then, \( \text{NL}_k(f) \geq \text{NL}_{T \cup S_1 \cup S_2}(f) \), and thus

\[
\text{nl}_2^{(n)} \geq \frac{n}{2} \binom{n/4 - 1}{i - 2} \left( 2\text{nl}_i^{(n/2)} - 2\binom{n/4 - 1}{i - 2} - 1 \right) + n \binom{n/4 - 1}{i - 2} \text{nl}_{i+1}^{(n/2)}.
\]

\[ \square \]

**Example 4.5** We use Construction-1 to design a 16-variable WPB function \( f \). Suppose that we choose an 8-variable WPB function \( g \) as the subfunction of \( f \) claimed in Construction-1, where \( g \) achieves the best weightwise nonlinearity profile in Example 3.13, i.e., \( \text{NL}_2(g) = 9 \), \( \text{NL}_3(g) = 22 \), \( \text{NL}_4(g) = 27 \). According to Theorem 4.4, if we set \( \text{nl}_2^{(8)} = 9 \), \( \text{nl}_3^{(8)} = 22 \), and \( \text{nl}_4^{(8)} = 27 \), then we obtain the lower bounds on \( \text{NL}_k(f), 3 \leq k \leq 8 \). See Table 2.

**Remark 4.6** Grain-128 [11] is a variant stream cipher selected in the eSTREAM project. It was shown in [4] that the employed 17-variable Boolean function \( h'(x) = x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus x_9 \oplus x_{10} \oplus x_{11} \oplus x_{12} \oplus x_{13} \oplus x_{14} \oplus x_{15} \oplus x_{16} \) of Grain-128 is not WPB, and thus is vulnerable to distinguish cryptanalysis when the attacker can access to the Hamming...
weight of the input of $h'$, especially for the weight larger than 8. The weightwise nonlinearity profile of $h'$ is also studied in [4]. Compared $h'$ with the 16-variable WPB function $f$ in Example 4.5, we conclude that

- for WPB property, $f$ provides the best resistance against distinguish attack,
- for $k$-weight nonlinearity, $f$ performs better than $h'$ if $k < 5$, and may be worse otherwise.

5 Concluding remarks

In this paper, we propose a large family of WPB functions over $\mathbb{F}_{2^n}$, where $n$ is a power of 2. These WPB functions are 2-rotation symmetric functions with algebraic degree $n - 1$, which are EA inequivalent to the known constructions. By employing the Krawtchouk polynomial, we give a method to calculate the weightwise nonlinearity of these functions. We also prove that the $k$-weight nonlinearity of these functions are always nonzero when $k$ is a positive power of 2. Moreover, we construct a subclass of WPB functions in our family, which have high weightwise nonlinearity profile. This is the first time that a class of Boolean functions achieving the best possible balancedness and high nonlinearity simultaneously with input restricted to constant weight vectors has been exhibited. Our work is beneficial in finding proper filter functions for homomorphic-friendly symmetric primitives like FLIP.

Acknowledgements The authors thank the anonymous reviewers for their valuable comments which have highly improved the manuscript.

References

1. Carlet C.: Boolean functions for cryptography and error correcting codes. In: Crama Y., Hammer P. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 257–397. Cambridge University Press, London (2010).
2. Carlet C.: Vectorial Boolean functions for cryptography. In: Crama Y., Hammer P. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 398–469. Cambridge University Press, London (2010).
3. Carlet C., Gao G., Liu W.: A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semi-bent functions. J. Comb. Theory A 127, 161–175 (2014).
4. Carlet C., Méaux P., Rotella Y.: Boolean functions with restricted input and their robustness; application to the FLIP cipher. IACR Trans. Symmetric Cryptol. 2017(3), 192–227 (2017).
5. Daemen J.: Cipher and hash function design strategies based on linear and differential cryptanalysis, PhD thesis, Catholic University of Louvain (1995).
6. Duval S., Lallemand V., Rotella Y.: Cryptanalysis of the FLIP family of stream ciphers. In: Advances in Cryptology—CRYPTO 2016, Lecture Notes in Computer Science, vol. 9814, pp. 457–475. Springer, Berlin (2016).
7. Filmus Y.: Friedgut-Kalai-Naor theorem for slices of the Boolean cube. Chicago J. Theor. Comput. Sci. 14, 1–17 (2016).
8. Filmus Y.: An orthogonal basis for functions over a slice of the Boolean hypercube. Electron. J. Comb. 23(1), 1–23 (2016).
9. Filmus Y., Mossel E.: Harmonicity and invariance on slices of the Boolean cube. In: 31st Conference on Computational Complexity, CCC 2016, pp. 1–16 (2016).
10. Filmus Y., Kindler G., Mossel E., Wimmer K.: Invariance principle on the slice. In: 31st Conference on Computational Complexity, CCC 2016, pp. 1–15 (2016).
11. Hell M., Johansson T., Maximov A., Meier W.: A stream cipher proposal: Grain-128. In: 2006 IEEE International Symposium on Information Theory, ISIT, pp. 1614–1618 (2006).
12. Joux A., Delaunay P.: Galois LFSR, embedded devices and side channel weaknesses. In: Progress in Cryptology—INDOCRYPT 2006, Lecture Notes in Computer Science, vol. 4329, pp. 436–451. Springer, Berlin (2006).
13. Kavut S.: Results on rotation-symmetric S-boxes. Inf. Sci. 201, 93–113 (2012).
14. Kavut S., Yücel M.D.: 9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class. Inf. Comput. 208(4), 341–350 (2010).
15. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. North-Holland Publishing Company, Amsterdam (1977).
16. Méaux P., Journault A., Standaert F.-X., Carlet C.: Towards stream ciphers for efficient FHE with low-noise ciphertexts, In: Advances in Cryptology—EUROCRYPT 2016, Lecture Notes in Computer Science, vol. 9665, pp. 311–343. Springer, Berlin (2016).
17. Mesnager S., Zhou Z., Ding C.: On the nonlinearity of Boolean functions with restricted input. Cryptogr. Commun. 1–14 (2018).
18. Su S., Tang X.: Systematic constructions of rotation symmetric bent functions, 2-rotation symmetric bent functions, and bent idempotent functions. IEEE Trans. Inf. Theory 63(7), 4658–4667 (2017).

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.