A NEW CONSTRUCTION OF WEIGHTWISE PERFECTLY BALANCED BOOLEAN FUNCTIONS

RUI ZHANG
School of Mathematics and Statistics
Henan University, Kaifeng, 475004, China

SIHONG SU*
School of Mathematics and Statistics
Henan University, Kaifeng, 475004, China
Henan Engineering Research Center for Artificial Intelligence Theory and Algorithms
Henan University, Kaifeng, 475004, China

(Communicated by Sihem Mesnager)

ABSTRACT. In this paper, we first introduce a class of quartic Boolean functions. And then, the construction of weightwise perfectly balanced Boolean functions on $2^m$ variables are given by modifying the support of the quartic functions, where $m$ is a positive integer. The algebraic degree, the weightwise nonlinearity, and the algebraic immunity of the newly constructed weightwise perfectly balanced functions are discussed at the end of this paper.

1. INTRODUCTION

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 [7]. 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. The symmetric primitive FLIP requires the Hamming weight of the key register to be invariant. An early version of FLIP faces an attack given by Duval et al. [3], which leads the design of the filter functions to become more complicated to reach better criteria on a subset of $\mathbb{F}_2^n$. In paper [1], 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.

Previous studies on Boolean functions with input restricted to constant weight vectors can be found in [4, 5]. Their work is asymptotical and from a probability point of view. The parameters, balancedness, and nonlinearity are strongly related to the resistance against the distinguishing attack and affine approximation attack, respectively. In 2017, Carlet, Méaux, and Rotella provided a security analysis on the

2020 Mathematics Subject Classification: Primary: 58F15, 58F17; Secondary: 53C35.
Key words and phrases: FLIP, Boolean functions, weightwise perfectly balancedness, algebraic degree, weightwise nonlinearity, algebraic immunity.

The second author is supported by the Key Scientific Research Project of Colleges and Universities in Henan Province (Grant No. 21A413003) and the National Natural Science Foundation of China (Grant No. 61502147).

* Corresponding author: Sihong Su (E-mail: sush@henu.edu.cn).
FLIP cipher and gave the first study on cryptographic criteria of Boolean functions with restricted input \[1\]. In paper \[9\], the authors studied the Boolean functions’ nonlinearity with restricted input.

Given an \(n\)-variable Boolean function \(f\), if for every integer \(k \in \{1, 2, \cdots, n-1\}\), the restriction of the function \(f\) to the subset \(E_{n,k} = \{ x \in \mathbb{F}_2^n | \text{wt}(x) = k \}\) is balanced and \(f(0,0,\cdots,0) \neq f(1,1,\cdots,1)\), then \(f\) is called weightwise perfectly balanced Boolean function, where \(\text{wt}(x)\) denotes the Hamming weight of the vector \(x \in \mathbb{F}_2^n\). In 2019, a large family of weightwise (almost) perfectly balanced Boolean functions with optimal algebraic immunity on \(\mathbb{F}_2^n\) and good algebraic immunity on some subsets of vectors in \(\mathbb{F}_2^n\), especially on the subsets of vectors with constant Hamming weight was proposed \[12\]. That was the first time that weightwise (almost) perfectly balanced Boolean functions with good local algebraic immunities are presented. In 2020, a class of weightwise perfectly balanced Boolean functions on \(2^{q+2}\) variables was constructed by modifying the support of a quadratic Boolean function \[6\], where \(q\) is a non-negative integer. In the same year, two methods of constructing weightwise perfectly balanced Boolean functions on \(2^k\) variables by modifying the support of a linear function and a quadratic function, respectively were proposed \[8\]. Furthermore, the authors also derived construction of \(n\)-variable weightwise almost perfectly balanced Boolean functions for any positive integer \(n\).

In 2021, the lower bound of the weightwise nonlinearity profile of a class of weightwise perfectly balanced Boolean functions on \(2^k\) variables was constructed by modifying the support of a linear function and a quadratic function, respectively was proposed \[11\]. That was the first time that weightwise (almost) perfectly balanced Boolean functions with good local algebraic immunities were presented. In 2020, a class of weightwise perfectly balanced Boolean functions on \(2^{q+2}\) variables was constructed by modifying the support of a quadratic Boolean function \[6\], where \(q\) is a non-negative integer. In the same year, two methods of constructing weightwise perfectly balanced Boolean functions on \(2^k\) variables by modifying the support of a linear function and a quadratic function, respectively were proposed \[8\]. Furthermore, the authors also derived construction of \(n\)-variable weightwise almost perfectly balanced Boolean functions for any positive integer \(n\).

In 2021, the lower bound of the weightwise nonlinearity profile of a class of weightwise perfectly balanced Boolean functions is determined in the paper \[11\].

In the present paper, we first give the construction of quartic functions on \(2^m\) variables, where \(m\) is an integer with \(m \geq 3\). Afterward, the construction of weightwise perfectly balanced Boolean functions is proposed by modifying the support of the quartic Boolean functions. Lastly, the algebraic degree, the weightwise nonlinearity, and the algebraic immunity of the newly constructed weightwise perfectly balanced functions are discussed.

The rest of this paper is organized as follows. Some basic definitions and necessary preliminaries are reviewed in Section 2. In Section 3, we present a class of quartic Boolean functions. The method of constructing weightwise perfectly balanced Boolean functions by modifying the support of the quartic Boolean functions is given in Section 4. The algebraic degree, the weightwise nonlinearity, and the algebraic immunity of these weightwise perfectly balanced Boolean functions are also studied. Section 5 concludes this paper.

2. Preliminaries

Let \(\mathbb{F}_2^n\) be the \(n\)-dimensional vector space over the finite field \(\mathbb{F}_2\) with two elements. Given a vector \(x = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n\), define its support as the set \(\text{supp}(x) = \{1 \leq i \leq n | x_i = 1\}\), and its Hamming weight as the cardinality of its support, i.e., \(\text{wt}(x) = |\text{supp}(x)|\). In this paper, for \(0 \leq k \leq n\), we always denote

\[
E_{n,k} = \{ x \in \mathbb{F}_2^n | \text{wt}(x) = k \}.
\]

Obviously, \(\bigcup_{k=0}^n E_{n,k} = \mathbb{F}_2^n\).

An \(n\)-variable Boolean function \(f\) is a mapping from \(\mathbb{F}_2^n\) into \(\mathbb{F}_2\). We denote by \(\mathcal{B}_n\) the set of all \(n\)-variable Boolean functions over \(\mathbb{F}_2^n\). The basic representation of an \(n\)-variable Boolean function \(f(x_1, x_2, \cdots, x_n)\), \((x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n\), is by the output of its truth table, i.e., a binary string of length \(2^n\) as

\[
f = [f(0,0,\cdots,0), f(1,0,\cdots,0), f(0,1,\cdots,0), \cdots, f(1,1,\cdots,1)]
\]
For a Boolean function $f \in \mathcal{B}_n$, its support is defined as supp$(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$. The Hamming weight of the Boolean function $f(x)$ is the cardinality of its support, i.e., wt$(f) = \mid$supp$(f)\mid$. The Hamming distance between two Boolean functions $f$ and $g$ on $n$ variables is the Hamming weight of $f \oplus g$, i.e., $d(f,g) = \text{wt}(f \oplus g)$. We say that a Boolean function $f$ on $n$ variables is balanced if wt$(f) = 2^{n-1}$. In cryptography, the algebraic normal form (ANF) of any $n$-variable Boolean function $f$ is defined as

$$f(x) = \bigoplus_{\mu \in \mathbb{F}_2^n} c_{\mu} x^{\mu} = \bigoplus_{\mu \in \mathbb{F}_2^n} c_{\mu} \prod_{i=1}^{n} x_{i}^{\mu_i},$$

where $c_{\mu} \in \mathbb{F}_2$, $x^{\mu} = \prod_{i=1}^{n} x_i^{\mu_i}$ for $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ and $\mu = (\mu_1, \mu_2, \ldots, \mu_n) \in \mathbb{F}_2^n$. The algebraic degree of an $n$-variable Boolean function $f$ in (2) is defined as

$$\text{deg}(f) = \max\{\text{wt}(\mu) \mid \mu \in \mathbb{F}_2^n, c_{\mu} = 1\}.$$  

If deg$(f) \leq 1$, then $f$ is called an affine function.

The algebraic immunity of a Boolean function expresses its ability to resist algebraic attack.

**Definition 2.1.** The algebraic immunity, denoted by $AI$, of a Boolean function $f(x)$ on $n$ variables is defined as

$$AI(f) = \min\{\text{deg}(g) \mid 0 \neq g \in \mathcal{B}_n \text{ such that } fg = 0 \text{ or } (f \oplus 1)g = 0\}.$$  

In fact, the algebraic immunity of an $n$-variable Boolean function $f$ satisfies $AI(f) \leq \lceil \frac{n}{2} \rceil$ (see [2]). If $AI(f) = \lceil \frac{n}{2} \rceil$, we say that the Boolean function $f$ has optimal algebraic immunity.

Denote by supp$_k(f)$ the support of a Boolean function $f \in \mathcal{B}_n$ on all the input with fixed Hamming weight $k$, i.e.,

$$\text{supp}_k(f) = \{x \in E_{n,k} \mid f(x) = 1\},$$

which is called the $k$-weight support of the Boolean function $f$, where $E_{n,k}$ is defined in (1) and $0 \leq k \leq n$. For convenience, denote

$$\text{zeros}_k(f) = \{x \in E_{n,k} \mid f(x) = 0\}.$$  

Further, denote

$$\text{wt}_k(f) = \mid \{x \in E_{n,k} \mid f(x) = 1\} \mid,$$

which is called the $k$-Hamming weight of the Boolean function $f$.

**Definition 2.2.** If a function $f \in \mathcal{B}_n$ satisfies $\text{wt}_k(f) = \frac{1}{2} \binom{n}{k}$ for every integer $k \in \{1, 2, \cdots, n-1\}$ and $f(0_n) \neq f(1_n)$, then $f$ is called the weightwise perfectly balanced (WPB) function.

Herein and hereafter, $0_n$ ($1_n$ resp.) is the vector of length $n$ in which all the coordinates are equal to 0 (1 resp.). The condition “$f(0_n) \neq f(1_n)$” makes $f$ globally balanced if the function $f$ satisfies $\text{wt}_k(f) = \frac{1}{2} \binom{n}{k}$ for $1 \leq k \leq n - 1$. Furthermore, it is proved that $n$-variable WPB Boolean functions exist only if $n$ is a power of 2 (see [1]). In this paper, we always consider the Boolean functions on $2^m$ variables, where $m$ is a positive integer.

Let $E$ be a subset of the vector space $\mathbb{F}_2^n$ and $f$ be an $n$-variable Boolean function restricted on $E$. The nonlinearity of the Boolean function $f$ on the subset $E$ is the minimum Hamming distance between the function $f$ and all the affine functions that are bound to $E$, denoted by $\text{NL}_E(f)$. In particular, the weightwise nonlinearity of
$f$ is defined as $NL_{E_n,k}(f)$ for $1 \leq k \leq n - 1$. The value of $NL_{E_n,k}(f)$ is called the $k$-weight nonlinearity of the function $f$, and will be denoted by $NL_k(f)$ if there is no risk of confusion.

**Proposition 1** ([1]). For every $n$-variable Boolean function $f$ over $\mathbb{F}_2^n$ and every subset $E$ of $\mathbb{F}_2^n$, we have

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

**Proposition 2** ([1]). Let $f$ be an $n$-variable Boolean function, and $\lfloor a \rfloor$ denote the maximum integer no larger than $a$. Then for every subset $E \subseteq \mathbb{F}_2^n$, we have

$$NL_E(f) \leq \left\lfloor \frac{|E|}{2} - \sqrt{|E|} \right\rfloor.$$

At the end of this section, we give two mathematical formulas as follows, which will be used in this paper.

**Lemma 2.3** ([13]). *(Pascal’s rule)* Given two integers $m$ and $p$, we have

$$\binom{m}{p} + \binom{m}{p+1} = \binom{m+1}{p+1}.$$ 

**Lemma 2.4** ([10]). *(Chu-Vandermonde’s identity)* Given three integers $p$, $q$, and $k$, we have

$$\sum_{j=0}^{k} \binom{p}{j} \binom{q}{k-j} = \binom{p+q}{k}.$$ 

### 3. A Quartic Boolean Function

In this section, a quartic Boolean function on $2^m$ variables is given, whose $k$-Hamming weight is determined for $0 \leq k \leq 2^m$, where $m$ is an integer with $m \geq 3$.

Let us define a $2^m$-variable Boolean function as

$$f_m(x) = \bigoplus_{i=1}^{2^{m-1}} x_i + \bigoplus_{i=1}^{2^{m-2}} x_i x_i + 2^{m-1} + \bigoplus_{i=1}^{2^{m-3}} x_i x_i x_i + 2^{m-2} x_i + 2^{m-1} x_i + 2^{m-2} x_i + 2^{m-1} + 2^m,$$

where $m \geq 3$ and $x = (x_1, x_2, \cdots, x_{2^m}) \in \mathbb{F}_2^{2^m}$.

**Example 1.** If $m = 3$, the 8-variable Boolean function defined in (5) is $f_3(x_1, x_2, \cdots, x_8) = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_1x_5 \oplus x_2x_6 \oplus x_1x_3x_5x_7$. Furthermore, the $k$-weight
supports of the function $f_3(x)$, $0 \leq k \leq 8$, are

\[
\begin{align*}
\text{supp}_0(f_3) &= \emptyset; \\
\text{supp}_1(f_3) &= \{1, 2, 4, 8\}; \\
\text{supp}_2(f_3) &= \{18, 20, 24, 33, 36, 40, 65, 66, 68, 72, 129, 130, 132, 136\}; \\
\text{supp}_3(f_3) &= \{7, 11, 13, 14, 19, 21, 25, 35, 38, 42, 52, 56, 82, 84, 88, 97, 100, 104, \\
&\quad 146, 148, 152, 161, 164, 168, 193, 194, 196, 200\}; \\
\text{supp}_4(f_3) &= \{30, 45, 53, 54, 57, 58, 71, 75, 77, 78, 83, 89, 99, 102, 106, 116, 120, \\
&\quad 135, 139, 141, 142, 147, 149, 153, 163, 166, 170, 180, 184, 210, 212, \\
&\quad 216, 225, 228, 232\}; \\
\text{supp}_5(f_3) &= \{31, 47, 55, 59, 87, 93, 94, 109, 118, 121, 122, 158, 173, 181, 182, 185, \\
&\quad 186, 199, 203, 205, 206, 211, 217, 227, 230, 234, 244, 248\}; \\
\text{supp}_6(f_3) &= \{111, 123, 125, 159, 175, 183, 187, 215, 221, 222, 237, 246, 249, 250\}; \\
\text{supp}_7(f_3) &= \{127, 239, 251, 253\}; \\
\text{supp}_8(f_3) &= \{255\},
\end{align*}
\]

where the vector $(x_1, x_2, \cdots, x_8)$ is written as $\sum_{i=1}^{8} x_i 2^{i-1} \in \{0, 1, \cdots, 255\}$.

It is easy to see that the 8-variable Boolean function $f_3(x)$ is WPB.

In order to calculate the $k$-Hamming weight of the quartic Boolean function $f_m(x)$ defined in (5), the following conclusions are very important.

**Lemma 3.1.** Given the $2^m$-variable Boolean function $f_m(x)$ defined in (5), we have

\[
f_m(x_1, x_2, \cdots, x_{2^m}) = f_{m-1}(x_1, x_3, \cdots, x_{2^m-1}) \oplus f_{m-1}(x_2, x_4, \cdots, x_{2^m}),
\]

where $m \geq 4$.

**Proof.** From the definition of $f_m(x)$ in (5), we have

\[
f_{m-1}(x_1, x_3, \cdots, x_{2^m-1}) = \bigoplus_{i=1}^{2^{m-2}} x_{2i-1} \oplus \bigoplus_{i=1}^{2^{m-3}} x_{2i-1} x_{2i-1+2^{m-1}} \oplus \bigoplus_{i=1}^{2^{m-4}} x_{2i-1} x_{2i-1+2^{m-2}} x_{2i-1+2^{m-1}} x_{2i-1+2^{m-2}+2^{m-2}},
\]

and

\[
f_{m-1}(x_2, x_4, \cdots, x_{2^m}) = \bigoplus_{i=1}^{2^{m-2}} x_{2i} \oplus \bigoplus_{i=1}^{2^{m-3}} x_{2i} x_{2i+2^{m-1}} \oplus \bigoplus_{i=1}^{2^{m-4}} x_{2i} x_{2i+2^{m-2}} x_{2i+2^{m-1}} x_{2i+2^{m-1}+2^{m-2}},
\]
Then, we get
\[
\begin{align*}
& f_{m-1}(x_1, x_3, \ldots, x_{2m-1}) \oplus f_{m-1}(x_2, x_4, \ldots, x_{2m}) \\
& = \bigoplus_{i=1}^{2^{m-2}} x_{2i-1} \oplus \bigoplus_{i=1}^{2^{m-3}} x_{2i-1}x_{2i-1+2^{m-1}} \oplus \bigoplus_{i=1}^{2^{m-4}} x_{2i-1}x_{2i-1+2^{m-2}}x_{2i-1+2^{m-1}} \oplus \bigoplus_{i=1}^{2^{m-3}} x_{2i} \oplus \bigoplus_{i=1}^{2^{m-2}} x_{2i}x_{2i+2^{m-1}} \oplus \bigoplus_{i=1}^{2^{m-3}} x_{2i}x_{2i+2^{m-1}}x_{2i+2^{m-1}}x_{2i+2^{m-2}} \oplus \\
& = \bigoplus_{i=1}^{2^{m-1}} x_i \oplus \bigoplus_{i=1}^{2^{m-2}} x_i x_{i+2^{m-1}} \oplus \bigoplus_{i=1}^{2^{m-3}} x_i x_{i+2^{m-2}}x_{i+2^{m-1}}x_{i+2^{m-1}}x_{i+2^{m-2}+2^{m-2}} \\
& = f_m(x_1, x_2, \ldots, x_{2m}).
\end{align*}
\]

The proof is completed. □

By Lemma 3.1, we can directly arrive at the following conclusion since \( f_m(x_1, x_2, \ldots, x_{2m}) = 1 \) if and only if \( f_{m-1}(x_1, x_3, \ldots, x_{2m-1}) \neq f_{m-1}(x_2, x_4, \ldots, x_{2m}) \). Hence, the \( k \)-weight support of the \( 2^m \)-variable Boolean function \( f_m(x) \) defined in (5), which is the support of the Boolean function \( f_m(x) \) with input restricted to \( E_{2m,k} \) defined in (1), is equal to

\[
\text{supp}_k(f_m) = \bigcup_{i=0}^{k} \{ x \in \mathbb{F}_2^{2m} \mid x' \in \text{supp}_i(f_{m-1}), x'' \in \text{zeros}_{k-i}(f_{m-1}) \} \cup \bigcup_{i=0}^{k} \{ x \in \mathbb{F}_2^{2m} \mid x' \in \text{zeros}_i(f_{m-1}), x'' \in \text{supp}_{k-i}(f_{m-1}) \},
\]

(6)

where \( x = (x_1, x_2, \ldots, x_{2m}) \), \( x' = (x_1, x_3, \ldots, x_{2m-1}) \), and \( x'' = (x_2, x_4, \ldots, x_{2m}) \).

**Lemma 3.2.** The \( k \)-Hamming weight of the \( 2^m \)-variable Boolean function \( f_m(x) \) defined in (5) satisfies

\[
\text{wt}_k(f_m) = 2^{m-1} \sum_{i=0}^{k} \text{wt}_i(f_{m-1}) \cdot \binom{2^{m-1}}{k-i} - \text{wt}_k(f_{m-1}),
\]

(7)

where \( 0 \leq k \leq 2^m \) and \( m \geq 3 \).

**Proof.** Assuming that \( k - i = j \), by (6), we have

\[
\text{supp}_k(f_m) = \bigcup_{i=0}^{k} \{ x \in \mathbb{F}_2^{2m} \mid x' \in \text{supp}_i(f_{m-1}), x'' \in \text{zeros}_{k-i}(f_{m-1}) \} \cup \bigcup_{j=0}^{k} \{ x \in \mathbb{F}_2^{2m} \mid x' \in \text{zeros}_{k-j}(f_{m-1}), x'' \in \text{supp}_j(f_{m-1}) \}
\]

\[
= \bigcup_{i=0}^{k} \{ x \in \mathbb{F}_2^{2m} \mid x' \in \text{supp}_i(f_{m-1}), x'' \in \text{zeros}_{k-i}(f_{m-1}) \} \cup \bigcup_{i=0}^{k} \{ x \in \mathbb{F}_2^{2m} \mid x'' \in \text{supp}_i(f_{m-1}), x' \in \text{zeros}_{k-i}(f_{m-1}) \},
\]
where \( x = (x_1, x_2, \cdots, x_{2^m}) \), \( x' = (x_1, x_3, \cdots, x_{2^m-1}) \), \( x'' = (x_2, x_4, \cdots, x_{2^m}) \), and 0 \( \leq k - j \leq k \) implies 0 \( \leq j \leq k \). Thus, we get
\[
\text{wt}_k(f_m) = |\text{supp}_k(f_m)| = 2 \sum_{i=0}^{k} \text{wt}_i(f_{m-1}) \left[ \binom{2^{m-1}}{k-i} - \text{wt}_{k-i}(f_{m-1}) \right].
\]

The proof is completed.

Furthermore, the following conclusion is also very important in the calculation of the k-Hamming weight of the \( 2^m \)-variable Boolean function \( f_m(x) \) defined in (5).

**Lemma 3.3.** Given two integers \( m \) and \( k \), we have
\[
\sum_{0 \leq i \leq k, \ k-i \equiv 0 \pmod{8}} \frac{1}{2} \binom{2^{m-1}}{i} \frac{(-1)^{\frac{k-i}{2}}}{2} \left( \frac{2^{m-1}}{8} \right)^{\frac{k-i}{8}} = \sum_{0 \leq i \leq k, \ i \equiv 0 \pmod{8}} \frac{1}{2} \binom{2^{m-1}}{k-i} \frac{(-1)^{\frac{i}{2}}}{2} \left( \frac{2^{m-1}}{8} \right)^{\frac{i}{8}}.
\]

**Proof.** Assuming that \( k - i = j \), we have
\[
\sum_{0 \leq i \leq k, \ k-i \equiv 0 \pmod{8}} \frac{1}{2} \binom{2^{m-1}}{i} \frac{(-1)^{\frac{k-i}{2}}}{2} \left( \frac{2^{m-1}}{8} \right)^{\frac{k-i}{8}} = \sum_{0 \leq j \leq k, \ j \equiv 0 \pmod{8}} \frac{1}{2} \binom{2^{m-1}}{k-j} \frac{(-1)^{\frac{j}{2}}}{2} \left( \frac{2^{m-1}}{8} \right)^{\frac{j}{8}} = \sum_{0 \leq i \leq k, \ i \equiv 0 \pmod{8}} \frac{1}{2} \binom{2^{m-1}}{k-i} \frac{(-1)^{\frac{i}{2}}}{2} \left( \frac{2^{m-1}}{8} \right)^{\frac{i}{8}}
\]

where 0 \( \leq k - j \leq k \) implies 0 \( \leq j \leq k \).

The proof is completed.

Now, the first main result of this paper is given as follows.

**Theorem 3.4.** The k-Hamming weight of the \( 2^m \)-variable Boolean function \( f_m(x) \) defined in (5) is equal to
\[
\text{wt}_k(f_m) = \begin{cases} 
\frac{1}{2} \binom{2^m}{k}, & k \not\equiv 0 \pmod{8}, \\
\frac{1}{2} \binom{2^m}{k} - (-1)^{\frac{k}{2}} \frac{2^m}{8}, & k \equiv 0 \pmod{8},
\end{cases}
\]

where 0 \( \leq k \leq 2^m \) and \( m \geq 3 \).

**Proof.** We use mathematical induction on \( m \) to finish the proof.

If \( m = 3 \), Example 1 shows that the conclusion is true, i.e., \( \text{wt}_0(f_3) = 0 \), \( \text{wt}_k(f_3) = \frac{1}{2} \binom{8}{k} \) for 1 \( \leq k \leq 7 \), and \( \text{wt}_8(f_3) = 1 \).

Now, let us prove that (9) is true when \( m \geq 4 \). Assume it is true for \( m-1 \), i.e.,
\[
\text{wt}_k(f_{m-1}) = \begin{cases} 
\frac{1}{2} \binom{2^{m-1}}{k}, & k \not\equiv 0 \pmod{8}, \\
\frac{1}{2} \binom{2^{m-1}}{k} - (-1)^{\frac{k}{2}} \frac{2^{m-1}}{8}, & k \equiv 0 \pmod{8},
\end{cases}
\]
where \(0 \leq k \leq 2^{m-1}\). Then, the \(k\)-Hamming weight of \(f_m\) is discussed according to the following two cases.

(1) When \(k \not\equiv 0 \pmod{8}\), it is easy to see that if \(i \equiv 0 \pmod{8}\) then \(k - i \not\equiv 0 \pmod{8}\), or if \(k - i \equiv 0 \pmod{8}\) then \(i \not\equiv 0 \pmod{8}\). By (7), we have

\[
\text{wt}_k(f_m) = 2 \sum_{i=0}^{k} \text{wt}_i(f_{m-1}) \left[\binom{2^{m-1}}{k-i} - \text{wt}_{k-i}(f_{m-1})\right]
\]

\[
= 2 \sum_{\substack{0 \leq i \leq k \atop i \not\equiv 0 \pmod{8}}} \left[\frac{1}{2} \binom{2^{m-1}}{i} \left[\binom{2^{m-1}}{k-i} - \frac{1}{2} \binom{2^{m-1}}{k-i}\right]\right] +
\]

\[
2 \sum_{\substack{0 \leq i \leq k \atop k - i \equiv 0 \pmod{8}}} \left[\frac{1}{2} \binom{2^{m-1}}{i} \left[\binom{2^{m-1}}{k-i} - \frac{1}{2} \binom{2^{m-1}}{k-i}\right] + \frac{(-1)^{k+i}}{2} \left(\frac{2^{m-1}}{8}\right)\right]
\]

\[
= 2 \sum_{\substack{0 \leq i \leq k \atop i \not\equiv 0 \pmod{8}}} \frac{1}{2} \binom{2^{m-1}}{i} \binom{2^{m-1}}{k-i} +
\]

\[
2 \sum_{\substack{0 \leq i \leq k \atop k - i \equiv 0 \pmod{8}}} \left[\frac{1}{2} \binom{2^{m-1}}{i} \binom{2^{m-1}}{k-i} + \frac{1}{2} \binom{2^{m-1}}{i} \frac{(-1)^{k+i}}{2} \left(\frac{2^{m-1}}{8}\right)\right]
\]

\[
= 2 \sum_{i=0}^{k} \frac{1}{2} \binom{2^{m-1}}{i} \frac{1}{2} \binom{2^{m-1}}{k-i} = \frac{1}{2} \binom{2^m}{k},
\]

where the second identity holds by (10), the fourth identity holds by (8), and the last identity holds by (4).

(2) When \(k \equiv 0 \pmod{8}\), it is easy to see that if \(i \equiv 0 \pmod{8}\) if and only if \(k - i \equiv 0 \pmod{8}\), or \(i \not\equiv 0 \pmod{8}\) if and only if \(k - i \not\equiv 0 \pmod{8}\). By (7), we have

\[
\text{wt}_k(f_m) = 2 \sum_{i=0}^{k} \text{wt}_i(f_{m-1}) \left[\binom{2^{m-1}}{k-i} - \text{wt}_{k-i}(f_{m-1})\right]
\]

\[
= 2 \sum_{\substack{0 \leq i \leq k \atop i \not\equiv 0 \pmod{8}}} \left[\frac{1}{2} \binom{2^{m-1}}{i} \left[\binom{2^{m-1}}{k-i} - \frac{1}{2} \binom{2^{m-1}}{k-i}\right]\right] +
\]

\[
2 \sum_{\substack{0 \leq i \leq k \atop k - i \equiv 0 \pmod{8}}} \left[\frac{1}{2} \binom{2^{m-1}}{i} \left[\binom{2^{m-1}}{k-i} - \frac{1}{2} \binom{2^{m-1}}{k-i}\right] + \frac{(-1)^{k+i}}{2} \left(\frac{2^{m-1}}{8}\right)\right]
\]

\[
= \frac{1}{2} \binom{2^m}{k},
\]
A new construction of weightwise perfectly balanced Boolean functions

In this section, we present the construction of WPB functions by modifying the support of the 2 variable Boolean function \( f \) defined in (5). The algebraic degree, the \( k \)-weight nonlinearity, and the algebraic immunity of the newly constructed WPB functions are also discussed.

4. Construction of WPB functions

From Theorem 3.4, we find that the 2\(^m\)-variable Boolean function \( f_m(x) \) defined in (5) is not a WPB function. So, we should modify the support of \( f_m(x) \) to get WPB functions.

For \( m \geq 1 \), define a 2\(^m\)-variable Boolean function as

\[
g_m(x) = \begin{cases} 
  x_1, & m = 1, \\
  x_1 \oplus x_2 \oplus x_1x_3, & m = 2, \\
  x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_1x_5 \oplus x_2x_6 \oplus x_1x_3x_5x_7, & m = 3, \\
  f_m(x) \oplus g_{m-3}(x') \prod_{i=1}^{2^{m-3}} \prod_{j=0}^{6} (x_{i+j2^{m-3}} \oplus x_{i+1(j+1)2^{m-3}} \oplus 1), & m \geq 4,
\end{cases}
\]

where \( x = (x_1, x_2, \cdots, x_{2^m}) \in \mathbb{F}_2^{2^m} \), \( x' = (x_1, x_2, \cdots, x_{2^m-3}) \), and \( f_m(x) \) is the 2\(^m\)-variable Boolean function defined in (5).

Note that 2\(^m\)-variable Boolean function \( \prod_{i=1}^{2^{m-3}} \prod_{j=0}^{6} (x_{i+j2^{m-3}} \oplus x_{i+1(j+1)2^{m-3}} \oplus 1) = 1 \) if and only if \( x_i = x_{i+2^{m-3}} = x_{i+2^{m-2}} = x_{i+2^{m-2}+2^{m-3}} = x_{i+2^{m-1}} = \cdots \).
where $m$ is an integer with $m \geq 4$, $0 \leq k \leq 2^m$, and $f_m(x)$ is the $2^m$-variable quartic Boolean function defined in (5).

Proof. According to the definition of the function $g_m(x)$ in (11), the $k$-weight support of the $2^m$-variable Boolean function $g_m(x)$ is discussed as follows.

1. When $k \not\equiv 0 \pmod{8}$, by (11), we have
\[
\text{supp}_k(g_m) = \text{supp}_k(f_m) \cup \{(x, x, x, x, x, x, x, x) \mid x \in \text{supp}_k(g_{m-3})\}
\]
where $A \cup B = (A \cup B) - (A \cap B)$ and the second identity holds by the fact that $\{(x, x, x, x, x, x, x, x) \mid x \in \text{supp}_k(g_{m-3})\} = \emptyset$ since $\frac{k}{8}$ is not an integer.

2. When $k \equiv 0 \pmod{8}$, we have
\[
\text{supp}_k(g_m) = \text{supp}_k(f_m) \cup \{(x, x, x, x, x, x, x, x) \mid x \in \text{supp}_k(g_{m-3})\} - \{(x, x, x, x, x, x, x, x) \mid x \in \text{supp}_k(g_{m-3}), f_m(x, x, x, x, x, x, x, x) = 1\}
\]
where the last identity holds since
\[
f_m(x, x, x, x, x, x, x, x) = f_m(x_1, x_2, \cdots, x_{2^m})
\]
\[
= \bigoplus_{i=1}^{2^{m-1}} x_i \bigoplus_{i=1}^{2^{m-2}} x_i x_{i+2^{m-1}} \bigoplus_{i=1}^{2^{m-3}} x_i x_{i+2^{m-2}} x_{i+2^{m-1}+2^{m-2}}
\]
\[
= \bigoplus_{i=1}^{M} (x_i \oplus x_{i+M} \oplus x_{i+2M} \oplus x_{i+3M}) \oplus \bigoplus_{i=1}^{M} (x_i x_{i+4M} \oplus x_{i+M} x_{i+5M})
\]
\[
= \bigoplus_{i=1}^{M} x_i x_{i+2M} x_{i+4M} x_{i+6M}
\]
\[
\equiv \text{wt}(x) \pmod{2}
\]
with $M = 2^{m-3}$, $x = (x_1, x_2, \ldots, x_M)$, $x_i = x_{i+M} = x_{i+2M} = \cdots = x_{i+7M}$ for $1 \leq i \leq M$, which gives $x_i \oplus x_{i+M} \oplus x_{i+2M} \oplus x_{i+3M} = 0$, $x_i x_{i+4M} \oplus x_{i+M} x_{i+5M} = 0$, and $x_i x_{i+2M} x_{i+4M} x_{i+6M} = x_i$ for $1 \leq i \leq M$.

The proof is completed. □

By Lemma 4.1 and (3), it is easy to get the following conclusion which will be used in the proof of the weightwise perfectly balancedness of the $2^m$-variable Boolean function $g_m(x)$ defined in (11).

**Corollary 1.** The $k$-Hamming weight of the $2^m$-variable Boolean function $g_m(x)$ defined in (11) is equal to

\[
\text{wt}_k(g_m) = \begin{cases} 
\text{wt}_k(f_m), & k \not\equiv 0 \pmod{8}, \\
\text{wt}_k(f_m) + \text{wt}_{k/8}(g_{m-3}) - 2\left|\left\{x \in \text{supp}_{k/8}(g_{m-3}) \mid \text{wt}(x) \text{ is odd}\right\}\right|, & k \equiv 0 \pmod{8},
\end{cases}
\]

where $m$ is an integer with $m \geq 4$, $0 \leq k \leq 2^m$, and $f_m(x)$ is the $2^m$-variable quartic Boolean function defined in (5).

Now, the second main result of this paper is given as follows.

**Theorem 4.2.** The $2^m$-variable Boolean function $g_m(x)$ defined in (11) is a WPB function, where $m$ is a positive integer.

**Proof.** We use mathematical induction on $m$ to finish the proof.

Firstly, it is easy to check that the functions $g_1$ and $g_2$ are WPB. Furthermore, the function $g_3$ is also WPB by Example 1 since $g_3 = f_3$.

Next, assume that $g_{m-3}(x)$ is a WPB function for $m \geq 4$, i.e.,

\[
\text{wt}_k(g_{m-3}) = \begin{cases} 
\frac{1}{2}
\begin{pmatrix} 2^m-3 \\ k \end{pmatrix}, & k \not\equiv 0 \pmod{8}, \\
\frac{1}{2}
\begin{pmatrix} 2^m \\ k \end{pmatrix}, & k \equiv 0 \pmod{8},
\end{cases}
\]

for $1 \leq k \leq 2^{m-3} - 1$, $\text{wt}_0(g_{m-3}) = 0$, and $\text{wt}_{2^{m-3}}(g_{m-3}) = 1$.

Thirdly, we calculate the $k$-Hamming weight of the function $g_m(x)$ for $m \geq 4$ and $0 \leq k \leq 2^m$ as follows.

(1) When $k \not\equiv 0 \pmod{8}$, by (12), the $k$-Hamming weight of the function $g_m(x)$ is equal to

\[
\text{wt}_k(g_m) = \text{wt}_k(f_m) \quad \text{and} \quad \text{wt}_k(g_m) = \begin{pmatrix} 2^m \\ k \end{pmatrix},
\]

where the second identity holds by (9).

(2) When $k \equiv 0 \pmod{8}$, by (12), the $k$-Hamming weight of the function $g_m(x)$ is equal to

\[
\text{wt}_k(g_m) = \text{wt}_k(f_m) + \text{wt}_{k/8}(g_{m-3}) - 2\left|\left\{x \in \text{supp}_{k/8}(g_{m-3}) \mid \text{wt}(x) \text{ is odd}\right\}\right|,
\]

which is discussed in the following subcases.
If $k/8$ is odd, then
\[
\text{wt}_k(g_m) = \text{wt}_k(f_m) + \text{wt}_{k/8}(g_{m-3}) - 2|\text{supp}_{k/8}(g_{m-3})| = \frac{1}{2} \binom{2^m}{k} - \frac{(-1)^{k/8}}{2} \binom{2^{m-3}}{k/8} + \frac{1}{2} \binom{2^{m-3}}{k/8} - 2 \times \frac{1}{2} \binom{2^{m-3}}{k/8} = \frac{1}{2} \binom{2^m}{k},
\]
where the first identity holds by the fact that if $x \in \text{supp}_{k/8}(g_{m-3})$ then $\text{wt}(x) = k/8$ and $k/8$ is odd, the second identity holds by (9), (13), and the fact that $|\text{supp}_{k/8}(g_{m-3})| = \text{wt}_{k/8}(g_{m-3})$, and the third identity holds since $k/8$ is odd.

If $k/8$ is even and $1 \leq k \leq 2^m - 1$, then
\[
\text{wt}_k(g_m) = \frac{1}{2} \binom{2^m}{k} - \frac{(-1)^{k/8}}{2} \binom{2^{m-3}}{k/8} + \frac{1}{2} \binom{2^{m-3}}{k/8} = \frac{1}{2} \binom{2^m}{k},
\]
where the first identity holds by the fact that \(\{x \in \text{supp}_{k/8}(g_{m-3}) | \text{wt}(x) \text{ is odd}\} = \emptyset\), the second identity holds by (9) and (13), and the third identity holds since $k/8$ is even.

If $k = 0$, then
\[
\text{wt}_0(g_m) = 0,
\]
since $\text{wt}_0(f_m) = \frac{1}{2} \binom{2^m}{k} - \frac{(-1)^{k/8}}{2} \binom{2^{m-3}}{k/8} = 0$ and $\text{wt}_0(g_{m-3}) = 0$.

If $k = 2^m$, which implies $k/8$ is even since $m \geq 4$, then
\[
\text{wt}_{2^m}(g_m) = 1,
\]
since $\text{wt}_{2^m}(f_m) = \frac{1}{2} \binom{2^m}{k} - \frac{(-1)^{k/8}}{2} \binom{2^{m-3}}{k/8} = 0$ and $\text{wt}_{2^m}(g_{m-3}) = 1$.

Thus, by Definition 2.2, we know the $2^m$-variable Boolean function $g_m(x)$ defined in (11) is WPB.

4.2. The algebraic degree, the $k$-weight nonlinearity and the algebraic immunity of the function $g_m$ in (11). 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.

**Theorem 4.3.** The algebraic degree of the $2^m$-variable WPB function $g_m(x)$ defined in (11) is equal to
\[
\deg(g_m) = \begin{cases} 
2^m - 1, & m \equiv 1 \pmod{3}, \\
2^m - 2, & m \equiv 2 \pmod{3}, \\
2^m - 4, & m \equiv 0 \pmod{3},
\end{cases}
\]
where \( m \geq 1 \).

**Proof.** We use mathematical induction on \( m \) to finish the proof.

By (11), we already know that \( \deg(g_1) = 1 \), \( \deg(g_2) = 2 \), and \( \deg(g_3) = 4 \). Hence, (14) is true for \( m = 1, 2, 3 \).

Now, let us prove that (14) is true for \( m \geq 4 \). Assume it is true for \( m - 3 \), i.e.,

\[
\deg(g_{m-3}) = \begin{cases} 
2^{m-3} - 1, & m \equiv 1 \pmod{3}, \\
2^{m-3} - 2, & m \equiv 2 \pmod{3}, \\
2^{m-3} - 4, & m \equiv 0 \pmod{3}.
\end{cases}
\]

Then, by (11), we have

\[
\deg(g_m) = \max\{\deg(f_m), \deg(g_{m-3}) + \deg(\prod_{i=1}^{2^{m-3}} \prod_{j=0}^{6}(x_{i+j}2^{m-3} + x_{i+(j+1)}2^{m-3} + 1))\}
\]

\[
= \deg(g_{m-3}) + \deg(\prod_{i=1}^{2^{m-3}} \prod_{j=0}^{6}(x_{i+j}2^{m-3} + x_{i+(j+1)}2^{m-3} + 1))
\]

\[
= \deg(g_{m-3}) + 7 \times 2^{m-3}
\]

\[
= \begin{cases} 
2^m - 1, & m \equiv 1 \pmod{3}, \\
2^m - 2, & m \equiv 2 \pmod{3}, \\
2^m - 4, & m \equiv 0 \pmod{3},
\end{cases}
\]

where the second identity holds by (5) since \( \deg(f_m) = 4 \) for \( m \geq 4 \).

The proof is completed. \( \square \)

Until now, we have not found an algorithm that can quickly calculate the \( k \)-weight nonlinearity and the algebraic immunity of the weightwise perfectly balanced Boolean function \( g_m \) defined in (11) on \( 2^m \) variables for any \( m = 1, 2, 3, \ldots \). Therefore, at the end of this subsection, we only calculate the \( k \)-weight nonlinearity and the algebraic immunity of the \( 2^m \)-variable weightwise perfectly balanced Boolean function \( g_m \) defined in (11) when \( m \) is relatively small by computer simulation. The \( k \)-weight nonlinearities of the function \( g_3 \) defined in (11) for \( k = 2, 3, 4, 5, 6 \) are given in Table 1, and the algebraic immunities of the function \( g_m \) in (11) for \( m = 2, 3, 4 \) are given in Table 2.

**Table 1.** The \( k \)-weight nonlinearity of \( g_3 \) in (11) for \( k = 2, 3, 4, 5, 6 \)

| \( k \) | \( k \)-weight nonlinearity of \( g_3 \) in (11) | \( \left(\frac{k}{3}\right)/2 - \frac{\binom{6}{k}}{2} \) |
|---|---|---|
| 2 | \( \text{NL}_2(g_3) = 2 \) | 11 |
| 3 | \( \text{NL}_3(g_3) = 12 \) | 24 |
| 4 | \( \text{NL}_4(g_3) = 19 \) | 30 |
| 5 | \( \text{NL}_5(g_3) = 12 \) | 24 |
| 6 | \( \text{NL}_6(g_3) = 6 \) | 11 |

From Table 1 and Table 2, we find that the \( k \)-weight nonlinearities of the WPB function \( g_3 \) defined in (11) and the algebraic immunities of the WPB function \( g_m \) in (11) for \( m = 2, 3, 4 \) are very poor. Therefore, we need to continue to work hard to construct WPB functions with better cryptographic properties in the future.
Table 2. The algebraic immunity of $g_m$ for $m = 2, 3, 4$

| $m$ | algebraic immunity of $g_m$ in (11) | optimal algebra immunity |
|-----|-------------------------------------|--------------------------|
| 2   | $AI(g_2) = 2$                       | 2                        |
| 3   | $AI(g_3) = 3$                       | 4                        |
| 4   | $AI(g_4) = 3$                       | 8                        |

5. Conclusion

In this paper, a class of quartic functions is proposed, which is used to construct WPB functions by modifying its support. The algebraic degree, the weightwise nonlinearity, and the algebraic immunity of the newly constructed WPB functions are considered at the end of this paper. How to create WPB functions with higher weightwise nonlinearity and higher algebraic immunity is our future work.

Acknowledgments

The authors would like to thank the associate editor and the anonymous reviewers for their constructive comments and suggestions which improved the quality of the paper.

References

[1] C. Carlet, P. Méaux and Y. Rotella, Boolean functions with restricted input and their robustness: Application to the FLIP cipher, IACR Trans. Symm. Cryptol., 2017 (2017), 192–227.
[2] N. T. Coutois and W. Meier, Algebraic attacks on stream ciphers with linear feedback, in Advances in Cryptology-EUROCRYPT 2003, 2656 (2003), 345–359.
[3] S. Duval, V. Lallemand and Y. Rotella, Cryptanalysis of the FLIP family of stream ciphers, in Advances in Cryptology—CRYPTO 2016, Lecture Notes in Computer Science, 9814, Berlin, Springer-Verlag, 2016, 457–475.
[4] Y. Filmus, Friedgut-Kalai-Naor theorem for slices of the Boolean cube, Chic. J. Theoret. Comput. Sci., 14 (2016), 1–17.
[5] Y. Filmus, An orthogonal basis for functions over a slice of the Boolean hypercube, Electron. J. Combin., 23 (2016), 1–23.
[6] J. Li and S. Su, Construction of weightwise perfectly balanced Boolean functions with high weightwise nonlinearity, Discr. Appl. Math., 279 (2020), 218–227.
[7] P. Méaux, A. Journault, F.-X. Standaert and C. Carlet, Towards stream ciphers for efficient FHE with low-noise ciphertexts, in Advances in Cryptology-EUROCRYPT 2016, Lecture Notes in Computer Science, 9665, Berlin, Springer-Verlag, 2016, 311–343.
[8] S. Mesnager and S. Su, On constructions of weightwise perfectly balanced Boolean functions, Cryptogr. Commun., (2021).
[9] S. Mesnager, Z. Zhou and C. Ding, On the nonlinearity of Boolean functions with restricted input, Cryptogr. Commun., 11 (2019), 63–76.
[10] A. Richard, Orthogonal polynomials and special functions, in Regional Conference Series in Applied Mathematics, 21, SIAM, Philadelphia, PA, 1975, 59–60.
[11] S. Su, The lower bound of the weightwise nonlinearity profile of a class of weightwise perfectly balanced functions, Discr. Appl. Math., 297 (2021), 60–70.
[12] D. Tang and J. Liu, A family of weightwise perfectly balanced boolean functions with optimal algebraic immunity, Cryptogr. Commun., 11 (2019), 1185–1197.
[13] E. W. Weisstein, Pascal’s formula, From MathWorld—A Wolfram Web Resource. Available from: http://mathworld.wolfram.com/PascalsFormula.html.

Received for publication January 2021.

E-mail address: 919957856@qq.com
E-mail address: sush@henu.edu.cn