mathematics

MDPI

Article

A New Construction of Weightwise Perfectly Balanced Functions with High Weightwise Nonlinearity

Qinglan Zhao [1,*], Yu Jia [1], Dong Zheng [1,2] and Baodong Qin [1]

[1] National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
[2] Westone Cryptologic Research Center (CRC), Chengdu 610095, China
* Correspondence: qinglan.zhao@xupt.edu.cn

Abstract: The FLIP cipher was proposed at Eurocrypt 2016 for the purpose of meliorating the efficiency of fully homomorphic cryptosystems. Weightwise perfectly balanced Boolean functions meet the balancedness requirement of the filter function in FLIP ciphers, and the construction of them has attracted serious attention from researchers. Nevertheless, the literature is still thin. Modifying the supports of functions with a low degree is a general construction technique whose key problem is to find a class of available low-degree functions. We first seek out a class of quadratic functions and then, based on these functions, present the new construction of weightwise perfectly balanced Boolean functions by adopting an iterative approach. It is worth mentioning that the functions we construct have good performance in weightwise nonlinearity. In particular, some p-weight nonlinearities achieve the highest values in the literature for a small number of variables.

Keywords: FLIP cipher; Boolean functions; weightwise perfectly balanced; weightwise nonlinearity

MSC: 06E30

Citation: Zhao, Q.; Jia, Y.; Zheng, D.; Qin, B. A New Construction of Weightwise Perfectly Balanced Functions with High Weightwise Nonlinearity. *Mathematics* **2023**, *11*, 1193. https://doi.org/10.3390/math11051193

Academic Editors: Ding Wang, Qi Jiang, Chunhua Su and Jonathan Blackledge

Received: 6 January 2023
Revised: 11 February 2023
Accepted: 24 February 2023
Published: 28 February 2023

1. Introduction

With the development of cloud services, the privacy protection of data stored in the cloud has become particularly important. One solution to providing secure cloud computing on untrusted public clouds is Fully Homomorphic Encryption. This encryption scheme supports the computation of encrypted data in a homomorphic way without needing decryption on the cloud. Cloud services based on FHE frameworks play a role in many applications, such as private data banks, encrypted search and multi-party security calculations, while they have the well-known bottlenecks: high computational cost and limited homomorphic capacity. See [1,2] for details.

To mitigate the bottlenecks and improve the efficiency of homomorphic encryption for an acceptable fully homomorphic cryptosystem, Méaux et al. [2] presented a new type of stream cipher, denoted as a filter permutator, at Eurocrypt 2016. They gave a general structure of filter permutators as shown in Figure 1 [2]. A filter permutator consists of three parts: the key register, which stores the original key; the permutation generator, which is parameterized by a Pseudo Random Number Generator (PRNG) and generates a permutation P to permute the key from the register; and the filter function, which filters the permuted key to output the key stream.

Lastly, the encryption (resp. decryption) needs to XOR the key stream with the plaintext (resp. ciphertext) to generate the ciphertext (resp. plaintext). A family of filter permutators, called FLIP, is specified. FLIP utilizes Knuth shuffle as the permutation generator parameterized by a forward secure PRNG based on the AES-128 and takes the direct sum of three Boolean functions as the filter function.

Different from the Boolean function used in traditional stream ciphers, the inputs of the Boolean function acting as a filter function in FLIP come from different permutations

of the same key and, therefore, have the same Hamming weight. As a result, in order to construct the filter function in FLIP, Boolean functions with restricted input, studied early in [3,4], have now become a class of functions of great interest in cryptography.

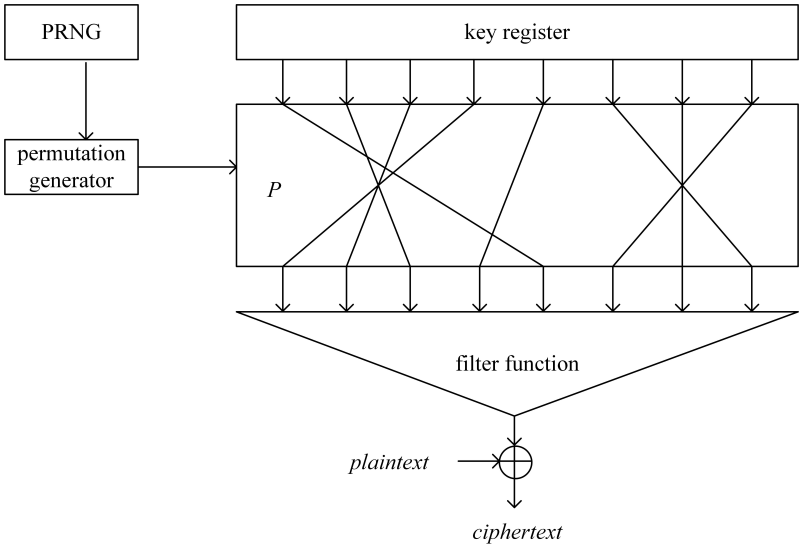

Figure 1. The general structure of filter permutators.

It has been shown that, for Boolean functions with restricted input, balancedness, nonlinearity and algebraic immunity continue to play a vital role in the corresponding attacks on somewhat homomorphic cryptosystems in the framework of FLIP ciphers (see [5,6]). Considering the first general cryptographic requirement, these functions need to be balanced. Therefore, weightwise perfectly balanced (WPB) Boolean functions become the focus of research on Boolean functions with restricted input.

If a Boolean function is always balanced when restricted to each subset of $\mathbb{F}_2^n$ with the same Hamming weight (not equal to 0 or n) and has different outputs when the input's Hamming weight is 0 and n, it is called a WPB function. In 2017, Carlet et al. constructed the first class of WPB functions using recursive methods for FLIP [6]. In 2019, the author in reference [7] proposed a class of WPB functions that belong to two-rotation symmetric Boolean functions. Some classes of WPB functions are presented by modifying the supports of Boolean functions with low algebraic degree not larger than 4 in [8–10].

The reference [11] analyzed the lower bound of weightwise nonlinearity of one class of WPB functions. A family of WPB functions with the maximal algebraic immunity is given in [12], and based on them, Mesnager et al. proposed two new concrete ones in 2022 [13]. Although WPB functions have attracted great attention, it is still challenging work to construct this class of functions, particularly the ones with other good cryptographic properties.

As mentioned above, modifying the supports of Boolean functions with low algebraic degree is a useful technique, which has been used in [8–10] to build WPB functions. The focus of this technique is to find low-degree functions. The authors in [8–10] found different functions possessing degrees not higher than 4. In this paper, we obtain a class of quadratic Boolean functions whose p-weight is easy to analyze and calculate. Utilizing these functions, we propose a fresh class of 2^m-variable WPB functions. We make a computer program and compute the p-weight nonlinearity of functions with a small number of variables. The experimental results show that our functions have significantly higher p-weight nonlinearity compared with the other main existing functions. In addition, we also analyze their algebraic degree and algebraic immunity.

The remainder of the paper is organized as follows. The formal definition and necessary preparations are introduced in Section 2. A class of quadratic Boolean functions is presented in Section 3. In Section 4, we give the construction of WPB functions and show

the specific process of proving them. Then, we compare the p-weight nonlinearity of WPB functions with other papers. Finally, we conclude the paper with Section 5.

2. Preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$, $x = (x_1, x_2, \ldots, x_n)$ be a vector in $\mathbb{F}_2^n$, all zero vector $0_n = (0, 0, \ldots, 0) \in \mathbb{F}_2^n$, and all one vector $1_n = (1, 1, \ldots, 1) \in \mathbb{F}_2^n$. The mapping f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is called an n-variable Boolean function. $\mathcal{B}_n$ is the set of all n-variable Boolean functions. Usually, f can be represented by its truth table, i.e.,

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

For a vector $x \in \mathbb{F}_2^n$, we claim its support $\mathrm{supp}(x)$ is $\{1 \le k \le n | x_k = 1\}$, and its Hamming weight $\mathrm{wt}(x)$ is $|\mathrm{supp}(x)|$. With being regarded as a vector, the Hamming weight of f is $\mathrm{wt}(f) = |\mathrm{supp}(f)|$, where f's support $\mathrm{supp}(f)$ is often described as the set of input vectors making f outputs 1—that is to say, $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n | f(x) = 1\}$. If $\mathrm{wt}(f)$ takes the value 2^{n-1}, we say that f is balanced.

In addition, f can be expressed by its algebraic normal form, i.e.,

$$f(x) = \bigoplus_{v \in \mathbb{F}_2^n} a_v x^v,$$

where the coefficient $a_v \in \mathbb{F}_2$, $x^v = x_1^{v_1} x_2^{v_2} \cdots x_n^{v_n}$. The algebraic degree of f is defined as

$$\deg(f) = max\{\mathrm{wt}(v) | v \in \mathbb{F}_2^n, a_v = 1\}.$$

A Boolean function f is said to be affine if $\deg(f) \le 1$.

When talking about a Boolean function f with restricted input, we define it is p-weight support as

$$\mathrm{supp}_p(f) = \{x \in \mathbb{F}_2^n | f(x) = 1, \mathrm{wt}(x) = p\},$$

where $0 \le p \le n$. The p-weight of f is

$$\mathrm{wt}_p(x) = \left|\mathrm{supp}_p(f)\right| = |\{x \in \mathrm{supp}(f) \mid \mathrm{wt}(x) = p\}|. \tag{1}$$

For the sake of argument, we denote $\mathrm{zeros}_p(f) = \{x \in \mathbb{F}_2^n | f(x) = 0, \mathrm{wt}(x) = p\}$.

Definition 1. *Let $f \in \mathcal{B}_n$. We claim that f is a WPB Boolean function if* $\mathrm{wt}_p(f) = \frac{1}{2}\binom{n}{p}$ *for* $1 \le p \le n-1$ *and* $f(0_n) \ne f(1_n)$.

Thus far, the existing research has indicated that the number of variables of the WPB Boolean function is a power of 2 [6]. Therefore, the Boolean functions that we construct in this paper have 2^m variables.

In addition to the consideration of balancedness, the construction of Boolean functions should also consider meeting high nonlinearity to achieve resistance against fast correlation attacks. Nonlinearity is a particularly important cryptographic criterion of Boolean functions, which describes the minimum Hamming distance between a Boolean function and all affine functions. When the input of a Boolean function is restricted to the vector set $\{x \in \mathbb{F}_2^n \mid \mathrm{wt}(x) = p\}$ with integer $p \le n$, we call its nonlinearity p-weight nonlinearity.

Definition 2. *Let $f \in \mathcal{B}_n$. For $0 \le p \le n$, the p-weight nonlinearity of f is expressed as*

$$\mathrm{NL}_p(f) = \frac{1}{2}\binom{n}{p} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \left| \sum_{x \in \mathbb{F}_2^n, \mathrm{wt}(x) = p} (-1)^{f(x) \oplus a \cdot x} \right|,$$

where $a \cdot x = a_1x_1 \oplus \cdots \oplus a_nx_n$. $\{\mathrm{NL}_1(f), \mathrm{NL}_2(f), ..., \mathrm{NL}_{n-1}(f)\}$ *is called the weightwise nonlinearity of* f.

Remarkably, reference [6] gives the upper bound of the p-weight nonlinearity of f as follows

$$\mathrm{NL}_p(f) \leq \left\lfloor \frac{1}{2}\binom{n}{p} - \frac{1}{2}\sqrt{\binom{n}{p}} \right\rfloor,$$

where $\lfloor a \rfloor$ is the largest integer not greater than a.

Another well-known cryptographic criterion of Boolean functions is algebraic immunity, which should be as high as possible to make the Boolean function resist algebraic attacks.

Definition 3. *Suppose* $f \in \mathcal{B}_n$. *The algebraic immunity of* f *is defined as*

$$\mathrm{AI}(f) = \min\{\deg(g) \mid g \in \mathrm{Ann}(f) \text{ or } \mathrm{Ann}(1 \oplus f)\},$$

where $\mathrm{Ann}(f) = \{g \mid 0 \neq g \in \mathcal{B}_n, fg = 0\}$.

Previous studies have shown that $\mathrm{AI}(f) \leq \lceil \frac{n}{2} \rceil$. Specially, if $\mathrm{AI}(f)$ reaches the value $\lceil \frac{n}{2} \rceil$, we say that f has the maximal algebraic immunity.

Next, we show the following two lemmas, which will be used later in the the paper.

Lemma 1. *(Pascal's Rule). Let k and j be two integers. We have*

$$\binom{k}{j} + \binom{k}{j+1} = \binom{k+1}{j+1}. \tag{2}$$

Lemma 2 ([14])**.** *(Chu–Vandermonde's Identity)). Let k,t and j be three integers. We have*

$$\sum_{i=0}^{j} \binom{k}{i}\binom{t}{j-i} = \binom{k+t}{j}. \tag{3}$$

3. Quadratic Functions

This section introduces a new class of quadratic functions, which is going to be utilized to construct the following WPB functions.

Let f_m be a 2^m-variable Boolean function with the form defined as

$$\begin{aligned} f_m(x_1, x_2, \ldots, x_{2^m}) =& x_1 \oplus x_2 \oplus \cdots \oplus x_{2^{m-1}} \\ & \oplus x_1x_{1+2^{m-2}} \oplus x_2x_{2+2^{m-2}} \oplus \cdots \oplus x_{2^{m-1}}x_{2^{m-1}+2^{m-2}}, \end{aligned} \tag{4}$$

where $m \geq 2$, $f_1 = x_1$.

Example 1. *If* $m = 2$, $f_2(x_1, x_2, x_3, x_4) = x_1 \oplus x_2 \oplus x_1x_2 \oplus x_2x_3$.
If $m = 3$, $f_3(x_1, x_2, \ldots, x_8) = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_1x_3 \oplus x_2x_4 \oplus x_3x_5 \oplus x_4x_6$.

Lemma 3. *For* $f_m(x)$ *defined in (4), it follows that*

$$f_m(x) = f_{m-1}(x') \oplus f_{m-1}(x''),$$

where $x = (x_1, x_2, \ldots, x_{2^m})$, $x' = (x_1, x_3, \ldots, x_{2^m-1})$, $x'' = (x_2, x_4, \ldots, x_{2^m})$, *and* $m \geq 3$.

Proof. By (4), it can be deduced that

$$\begin{aligned} f_{m-1}(x') =& x_1 \oplus x_3 \oplus \cdots \oplus x_{2^{m-1}-1} \oplus \\ & x_1x_{1+2^{m-2}} \oplus x_3x_{3+2^{m-2}} \oplus \cdots \oplus x_{2^{m-1}-1}x_{2^{m-1}-1+2^{m-2}}, \end{aligned}$$

and

$$\begin{aligned} f_{m-1}(x'') =& x_2 \oplus x_4 \oplus \cdots \oplus x_{2^{m-1}} \oplus \\ & x_2 x_{2+2^{m-2}} \oplus x_4 x_{4+2^{m-2}} \oplus \cdots \oplus x_{2^{m-1}} x_{2^{m-1}+2^{m-2}}. \end{aligned}$$

Then, we obtain

$$\begin{aligned} f_{m-1}(x') \oplus f_{m-1}(x'') =& x_1 \oplus x_2 \oplus \cdots \oplus x_{2^{m-1}} \\ & \oplus x_1 x_{1+2^{m-2}} \oplus x_2 x_{2+2^{m-2}} \oplus \cdots \oplus x_{2^{m-1}} x_{2^{m-1}+2^{m-2}} \\ =& f_m(x). \end{aligned}$$

□

By Lemma 3, we can easily know that $f_m(x) = 1$ if and only if $f_{m-1}(x') \neq f_{m-1}(x'')$, where x' and x'' are defined as same as in Lemma 3. The p-weight support of f_m in (4) can be derived from this fact, which is

$$\begin{aligned} \mathrm{supp}_p(f_m) = & \bigcup_{i=0}^{p} \left\{ x \in \mathbb{F}_2^{2^m} \mid x' \in \mathrm{supp}_i(f_{m-1}), x'' \in \mathrm{zeros}_{p-i}(f_{m-1}) \right\} \cup \\ & \bigcup_{i=0}^{p} \left\{ x \in \mathbb{F}_2^{2^m} \mid x' \in \mathrm{zeros}_i(f_{m-1}), x'' \in \mathrm{supp}_{p-i}(f_{m-1}) \right\}. \end{aligned} \tag{5}$$

Lemma 4. *The p-weight of f_m defined in (4) is*

$$\mathrm{wt}_p(f_m) = 2 \sum_{i=0}^{p} \mathrm{wt}_i(f_{m-1}) \left[\binom{2^{m-1}}{p-i} - \mathrm{wt}_{p-i}(f_{m-1}) \right], \tag{6}$$

where $1 \leq p \leq 2^m - 1$ and $m \geq 3$.

Proof. Assuming that $p - i = j$, from (5), we have

$$\begin{aligned} \mathrm{supp}_p(f_m) = & \bigcup_{i=0}^{p} \left\{ x \in \mathbb{F}_2^{2^m} \mid x' \in \mathrm{supp}_i(f_{m-1}), x'' \in \mathrm{zeros}_{p-i}(f_{m-1}) \right\} \cup \\ & \bigcup_{j=0}^{p} \left\{ x \in \mathbb{F}_2^{2^m} \mid x' \in \mathrm{zeros}_{p-j}(f_{m-1}), x'' \in \mathrm{supp}_j(f_{m-1}) \right\} \\ = & \bigcup_{i=0}^{p} \left\{ x \in \mathbb{F}_2^{2^m} \mid x' \in \mathrm{supp}_i(f_{m-1}), x'' \in \mathrm{zeros}_{p-i}(f_{m-1}) \right\} \cup \\ & \bigcup_{i=0}^{p} \left\{ x \in \mathbb{F}_2^{2^m} \mid x'' \in \mathrm{supp}_i(f_{m-1}), x' \in \mathrm{zeros}_{p-i}(f_{m-1}) \right\}, \end{aligned}$$

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

$$\mathrm{wt}_p(f_m) = |\mathrm{supp}_p(f_m)| = 2 \sum_{i=0}^{p} \mathrm{wt}_i(f_{m-1}) \left[\binom{2^{m-1}}{p-i} - \mathrm{wt}_{p-i}(f_{m-1}) \right].$$

□

Lemma 5. *Suppose m and p are two integers, then we have*

$$\begin{aligned}&\sum_{\substack{0\le i\le p\\ (p-i)\ is\ even}}\frac{1}{2}\binom{2^{m-1}}{i}\frac{(-1)^{\frac{p-i}{2}}}{2}\binom{2^{m-2}}{\frac{p-i}{2}}\\ =&\sum_{\substack{0\le i\le p\\ i\ is\ even}}\frac{1}{2}\binom{2^{m-1}}{p-i}\frac{(-1)^{\frac{i}{2}}}{2}\binom{2^{m-2}}{\frac{i}{2}}.\end{aligned}\tag{7}$$

Proof. Assuming that $p-i=j$, we have

$$\begin{aligned}&\sum_{\substack{0\le i\le p\\ (p-i)\text{ is even}}}\frac{1}{2}\binom{2^{m-1}}{i}\frac{(-1)^{\frac{p-i}{2}}}{2}\binom{2^{m-2}}{\frac{p-i}{2}}\\ =&\sum_{\substack{0\le j\le p\\ j\text{ is even}}}\frac{1}{2}\binom{2^{m-1}}{p-j}\frac{(-1)^{\frac{j}{2}}}{2}\binom{2^{m-2}}{\frac{j}{2}}\\ =&\sum_{\substack{0\le i\le p\\ i\text{ is even}}}\frac{1}{2}\binom{2^{m-1}}{p-i}\frac{(-1)^{\frac{i}{2}}}{2}\binom{2^{m-2}}{\frac{i}{2}}.\end{aligned}$$

□

Theorem 1. *The p-weight of f_m defined in (4) is*

$$\mathrm{wt}_p(f_m)=\begin{cases}\frac{1}{2}\binom{2^m}{p}, & p\not\equiv 0(\mathrm{mod}2),\\ \frac{1}{2}\binom{2^m}{p}-\frac{(-1)^{\frac{p}{2}}}{2}\binom{2^{m-1}}{\frac{p}{2}}, & p\equiv 0(\mathrm{mod}2),\end{cases}\tag{8}$$

where $1\le p\le 2^m-1$ and $m\ge 2$.

Proof. When $m=2$, the p-weights of $f_2(x_1,x_2,x_3,x_4)=x_1\oplus x_2\oplus x_1x_2\oplus x_2x_3$ in (4) are

$$\mathrm{wt}_1(f)=\frac{1}{2}\binom{4}{1}=2,\mathrm{wt}_2(f)=\frac{1}{2}\binom{4}{2}+1=4,\mathrm{wt}_3(f)=\frac{1}{2}\binom{4}{3}=2.$$

Thus, the p-weights of f_2 clearly satisfy (8).

The p-weights of the Boolean function $f_3(x_1,x_2,\ldots,x_8)=x_1\oplus x_2\oplus x_3\oplus x_4\oplus x_1x_3\oplus x_2x_4\oplus x_3x_5\oplus x_4x_6$ when $m=3$ in (4) are given in Table 1. It is easy to see that all the p-weights of f_3 satisfy (8).

Table 1. The p-weights of f_3 defined in (4).

p	1	2	3	4	5	6	7
$\mathrm{wt}_p(f_3)$	4	16	28	32	28	16	4
$\frac{1}{2}\binom{8}{p}$	4	14	28	35	28	14	4

Now, we will use mathematical induction to complete this proof. We first assume that (8) holds for f_{m-1} when $m\ge 3$, i.e.,

$$\mathrm{wt}_p(f_{m-1})=\begin{cases}\frac{1}{2}\binom{2^{m-1}}{p}, & p\not\equiv 0(\mathrm{mod}2),\\ \frac{1}{2}\binom{2^{m-1}}{p}-\frac{(-1)^{\frac{p}{2}}}{2}\binom{2^{m-2}}{\frac{p}{2}}, & p\equiv 0(\mathrm{mod}2).\end{cases}\tag{9}$$

In what follows, we prove that (8) holds for f_m.

(1) When p is a odd, it can be easily deduced that $p-i$ is even if i is odd, or that $p-i$ is odd if i is even. Then, we have

$$\begin{aligned}
&\mathrm{wt}_p(f_m)\\
&= 2\sum_{i=0}^{p}\mathrm{wt}_i(f_{m-1})\left[\binom{2^{m-1}}{p-i}-\mathrm{wt}_{p-i}(f_{m-1})\right]\\
&= 2\sum_{\substack{0\le i\le p\\ i \text{ is even}}}\left[\frac{1}{2}\binom{2^{m-1}}{i}-\frac{(-1)^{\frac{i}{2}}}{2}\binom{2^{m-2}}{\frac{i}{2}}\right]\frac{1}{2}\binom{2^{m-1}}{p-i}+\\
&\quad 2\sum_{\substack{0\le i\le p\\ i \text{ is odd}}}\frac{1}{2}\binom{2^{m-1}}{i}\left[\frac{1}{2}\binom{2^{m-1}}{p-i}+\frac{(-1)^{\frac{p-i}{2}}}{2}\binom{2^{m-2}}{\frac{p-i}{2}}\right]\\
&= 2\sum_{\substack{0\le i\le p\\ i \text{ is even}}}\left[\frac{1}{2}\binom{2^{m-1}}{i}\frac{1}{2}\binom{2^{m-1}}{p-i}-\frac{1}{2}\binom{2^{m-1}}{p-i}\frac{(-1)^{\frac{i}{2}}}{2}\binom{2^{m-2}}{\frac{i}{2}}\right]+\\
&\quad 2\sum_{\substack{0\le i\le p\\ i \text{ is odd}}}\left[\frac{1}{2}\binom{2^{m-1}}{i}\frac{1}{2}\binom{2^{m-1}}{p-i}+\frac{1}{2}\binom{2^{m-1}}{i}\frac{(-1)^{\frac{p-i}{2}}}{2}\binom{2^{m-2}}{\frac{p-i}{2}}\right]\\
&= 2\sum_{i=0}^{p}\frac{1}{2}\binom{2^{m-1}}{i}\frac{1}{2}\binom{2^{m-1}}{p-i}\\
&= \frac{1}{2}\binom{2^m}{p},
\end{aligned}$$

where the first, second and fourth equations hold due to (6), (9) and (7), respectively, and the last one is from fact (3).

(2) When p is even, we find that i is odd if $p-i$ is odd, or that i is even if $p-i$ is even. Then, we have

$$\begin{aligned}
&\mathrm{wt}_p(f_m)\\
&= 2\sum_{i=0}^{p}\mathrm{wt}_i(f_{m-1})\left[\binom{2^{m-1}}{p-i}-\mathrm{wt}_{p-i}(f_{m-1})\right]\\
&= 2\sum_{\substack{0\le i\le p\\ i \text{ is even}}}\left[\frac{1}{2}\binom{2^{m-1}}{i}-\frac{(-1)^{\frac{i}{2}}}{2}\binom{2^{m-2}}{\frac{i}{2}}\right]\left[\frac{1}{2}\binom{2^{m-1}}{p-i}+\frac{(-1)^{\frac{p-i}{2}}}{2}\binom{2^{m-2}}{\frac{p-i}{2}}\right]\\
&\quad +2\sum_{\substack{0\le i\le p\\ i \text{ is odd}}}\frac{1}{2}\binom{2^{m-1}}{i}\left[\binom{2^{m-1}}{p-i}-\frac{1}{2}\binom{2^{m-1}}{p-i}\right]\\
&= 2\sum_{\substack{0\le i\le p\\ i \text{ is even}}}\left[\frac{1}{2}\binom{2^{m-1}}{i}\frac{1}{2}\binom{2^{m-1}}{p-i}-\frac{(-1)^{\frac{i}{2}}}{2}\binom{2^{m-2}}{\frac{i}{2}}\frac{(-1)^{\frac{p-i}{2}}}{2}\binom{2^{m-2}}{\frac{p-i}{2}}\right]\\
&\quad +2\sum_{\substack{0\le i\le p\\ i \text{ is odd}}}\frac{1}{2}\binom{2^{m-1}}{i}\frac{1}{2}\binom{2^{m-1}}{p-i}\\
&= 2\sum_{i=0}^{p}\frac{1}{2}\binom{2^{m-1}}{i}\frac{1}{2}\binom{2^{m-1}}{p-i}-2\sum_{\substack{0\le i\le p\\ i \text{ is even}}}\frac{(-1)^{\frac{i}{2}}}{2}\binom{2^{m-2}}{\frac{i}{2}}\frac{(-1)^{\frac{p-i}{2}}}{2}\binom{2^{m-2}}{\frac{p-i}{2}}\\
&= \frac{1}{2}\binom{2^m}{p}-\frac{(-1)^{\frac{p}{2}}}{2}\binom{2^{m-1}}{\frac{p}{2}},
\end{aligned}$$

where the first, second and fourth equations hold due to (6), (9) and (7), respectively, and the last one is from fact (3).

□

4. WPB Functions

Let h_m be a 2^m-variable Boolean function, which can be defined as

$$h_m(x) = f_m(x) \oplus h_{m-1}(\overline{x}) \prod_{i=1}^{2^{m-1}} (x_i \oplus x_{2^{m-1}+i} \oplus 1), \tag{10}$$

where $m \geq 2$, $x = (x_1, x_2, ..., x_{2^m}) \in \mathbb{F}_2^{2^m}$, $\overline{x} = (x_1, x_2, ..., x_{2^{m-1}}) \in \mathbb{F}_2^{2^{m-1}}$, $h_1 = x_1$, and $f_m(x)$ is defined in (4).

Example 2. *It is clear that h_1 is WPB. When $m = 2$, then*

$$h_2(x_1, x_2, x_3, x_4) = x_1 \oplus x_2 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_2x_3 \oplus x_1x_3x_4.$$

The p-weight supports of h_2 are as follows,

$$\begin{aligned}
&\mathrm{supp}_0(h_2) = \varnothing,\\
&\mathrm{supp}_1(h_2) = \{(1,0,0,0),(0,1,0,0)\},\\
&\mathrm{supp}_2(h_2) = \{(1,1,0,0),(0,1,0,1),(1,0,0,1)\},\\
&\mathrm{supp}_3(h_2) = \{(1,1,0,1),(1,0,1,1)\},\\
&\mathrm{supp}_4(h_2) = \{(1,1,1,1)\}.
\end{aligned}$$

Thus, h_2 is WPB acoording the definition of WPB functions.

Lemma 6. *Let f_m be defined in (4). Given a vector $x = (x_1, x_2, ..., x_{2^m}) \in \mathbb{F}_2^{2^m}$ such that $x_i = x_{2^{m-1}+i}$ for all $1 \leq i \leq 2^{m-1}$, we have $f_m(x) = \mathrm{wt}(\overline{x}) (\mathrm{mod}\, 2)$, where $\overline{x} = (x_1, x_2, ..., x_{2^{m-1}}) \in \mathbb{F}_2^{2^{m-1}}$.*

Proof.

$$\begin{aligned}
& f_m(x)\\
=\ & x_1 \oplus x_2 \oplus \cdots \oplus x_{2^{m-1}} \oplus x_1x_{1+2^{m-2}} \oplus x_2x_{2+2^{m-2}} \oplus \cdots \oplus x_{2^{m-2}}x_{2^{m-1}}\\
& \oplus x_{2^{m-2}+1}x_{2^{m-1}+1} \oplus x_{2^{m-2}+2}x_{2^{m-1}+2} \oplus \cdots \oplus x_{2^{m-1}}x_{2^{m-1}+2^{m-2}}\\
=\ & x_1 \oplus x_2 \oplus \cdots \oplus x_{2^{m-1}} \oplus x_1x_{1+2^{m-2}} \oplus x_2x_{2+2^{m-2}} \oplus \cdots \oplus x_{2^{m-2}}x_{2^{m-1}}\\
& \oplus x_{2^{m-2}+1}x_1 \oplus x_{2^{m-2}+2}x_2 \oplus \cdots \oplus x_{2^{m-1}}x_{2^{m-2}}\\
=\ & x_1 \oplus x_2 \oplus \cdots \oplus x_{2^{m-1}}\\
=\ & \mathrm{wt}(\overline{x}) (\mathrm{mod}\, 2),
\end{aligned}$$

where $\overline{x} = \{x_1, x_2, ..., x_{2^{m-1}}\}$. □

When $m \geq 2$, we note two facts: (1) the 2^m-variable function $\prod_{i=1}^{2^{m-1}} (x_i \oplus x_{2^{m-1}+i} \oplus 1)$ takes 1 if and only if $x_i = x_{2^{m-1}+i}$ for all $1 \leq i \leq 2^{m-1}$, and (2) $h_m = 1$ if and only if $f_m \neq h_{m-1} \prod_{i=1}^{2^{m-1}} (x_i \oplus x_{2^{m-1}+i} \oplus 1)$. Therefore, we have come to the following conclusion.

Corollary 1. *The p-weight support of Boolean function $h_m(x)$ defined in (10) is*

$$\begin{aligned}
\mathrm{supp}_p(h_m) = & \mathrm{supp}_p(f_m) \cup \left\{ (\overline{x}, \overline{x}) \mid \overline{x} \in \mathrm{supp}_{\frac{p}{2}}(h_{m-1}) \right\}\\
& \setminus \left\{ (\overline{x}, \overline{x}) \mid \overline{x} \in \mathrm{supp}_{\frac{p}{2}}(h_{m-1}), \mathrm{wt}(\overline{x}) \textit{ is odd} \right\},
\end{aligned} \tag{11}$$

where $m \geq 2$, $x = (x_1, x_2, \ldots, x_{2^m}) \in \mathbb{F}_2^{2^m}$, $\overline{x} \in \mathbb{F}_2^{2^{m-1}}$, $f_m(x)$ *is defined in* (4), *and* $1 \leq p \leq 2^m - 1$.

Theorem 2. h_m *defined in* (10) *is a weightwise perfectly balanced function.*

Proof. We use mathematical induction on m in the proof process. First, by Example 2, we learn that h_1 and h_2 are WPB functions. Next, we assume that h_{m-1} is a WPB function for $m \geq 3$ with $h_{m-1}(0_{m-1}) = 0$ and $h_{m-1}(1_{m-1}) = 1$. Thus, for $1 \leq p \leq 2^{m-1} - 1$,

$$\mathrm{wt}_p(h_{m-1}) = \frac{1}{2}\binom{2^{m-1}}{p}. \tag{12}$$

The calculation of the p-weight of $h_m(x)$ defined in (10) is divided into three specific cases according to the value of p.

(1) If p is odd, we claim $\prod_{i=1}^{2^{m-1}}(x_i \oplus x_{2^{m-1}+i} \oplus 1) = 0$, and then

$$\mathrm{wt}_p(h_m) = \mathrm{wt}_p(f_m) = \frac{1}{2}\binom{2^m}{p},$$

where the last identity holds by Theorem 1.

(2) If p is even, there is one case where there is an integer i such that x_i is not equal to $x_{2^{m-1}+i}$. In this case, $\mathrm{wt}_p(h_m) = \frac{1}{2}\binom{2^m}{p}$, similarly to case (1). There is another case where the fact holds that $x_i = x_{2^{m-1}+i}$ for all $1 \leq i \leq 2^{m-1}$. In this case, we will discuss the p-weight of $h_m(x)$ on the basis of the parity of $\frac{p}{2}$.

(2-1) If $\frac{p}{2}$ is odd, we claim

$$\begin{aligned}
\mathrm{wt}_p(h_m) &= \left|x \in \mathrm{supp}_p(h_m)\right| \\
&= \left|\mathrm{supp}_p(f_m)\right| + \left|\mathrm{supp}_{\frac{p}{2}}(h_{m-1})\right| - 2\left|\left\{\overline{x} \in \mathrm{supp}_{\frac{p}{2}}(h_{m-1}) \mid \mathrm{wt}(\overline{x}) \text{ is odd}\right\}\right| \\
&= \frac{1}{2}\binom{2^m}{p} - \frac{(-1)^{\frac{p}{2}}}{2}\binom{2^{m-1}}{\frac{p}{2}} + \frac{1}{2}\binom{2^{m-1}}{\frac{p}{2}} - 2 \times \frac{1}{2}\binom{2^{m-1}}{\frac{p}{2}} \\
&= \frac{1}{2}\binom{2^m}{p},
\end{aligned}$$

where $x \in \mathbb{F}_2^{2^m}$, $\overline{x} \in \mathbb{F}_2^{2^{m-1}}$. The second equality can be derived from Corollary 1, the third equality holds due to (8) and (12), and the last equality holds because $\frac{p}{2}$ is odd.

(2-2) If $\frac{p}{2}$ is even, we claim

$$\begin{aligned}
\mathrm{wt}_p(h_m) &= \left|x \in \mathrm{supp}_p(h_m)\right| \\
&= \left|\mathrm{supp}_p(f_m)\right| + \left|\mathrm{supp}_{\frac{p}{2}}(h_{m-1})\right| - 2\left|\left\{\overline{x} \in \mathrm{supp}_{\frac{p}{2}}(h_{m-1}) \mid \mathrm{wt}(\overline{x}) \text{ is odd}\right\}\right| \\
&= \frac{1}{2}\binom{2^m}{p} - \frac{(-1)^{\frac{p}{2}}}{2}\binom{2^{m-1}}{\frac{p}{2}} + \frac{1}{2}\binom{2^{m-1}}{\frac{p}{2}} \\
&= \frac{1}{2}\binom{2^m}{p},
\end{aligned}$$

where $x \in \mathbb{F}_2^{2^m}$, $\overline{x} \in \mathbb{F}_2^{2^{m-1}}$. The second equation holds because of Corollary 1, the third equation is given by (8) and (12), and the last equation holds because of the condition that $\frac{p}{2}$ is even.

Now, we consider the vectors 0_{2^m} and 1_{2^m}. It is easy to see that $h_m(0_{2^m}) = 0$, and $h_m(1_{2^m}) = 1$ since $f_m(1_{2^m}) = 0$, $h_{m-1}(1_{2^{m-1}}) = 1$.

Based on the above discussion, the result follows that $h_m(x)$ defined in (10) is a WPB function. □

Theorem 3. *The algebraic degree of WPB function $h_m(x)$ defined in (10) is*

$$\deg(h_m) = 2^m - 1.$$

Proof. Let the 2^m-variable Boolean fuction $g_m(x) = h_{m-1}(\overline{x}) \prod_{i=1}^{2^{m-1}} (x_i \oplus x_{2^{m-1}+i} \oplus 1)$, where $\overline{x} \in \mathbb{F}_2^{2^{m-1}}$. Since $\deg(h_m) = \max\{\deg(f_m), \deg(g_m)\}$, we can easily obtain $\deg(h_m) = \deg(g_m)$.

Based on the obvious fact that $\deg(h_1) = 1$ and $\deg(h_2) = 3$, we assume $\deg(h_{m-1}) = 2^{m-1} - 1$. Then, we have

$$\deg(h_m) = \deg(g_m) = 2^{m-1} - 1 + 2^{m-1} = 2^m - 1.$$

□

We simulate the p-weight nonlinearity of h_3 and h_4 using the computer program and compare them with existing WPB functions. As shown in Tables 2 and 3, the p-weight nonlinearity of h_3 and h_4 are close to the upper bound $\left\lfloor \frac{1}{2}\binom{n}{p} - \frac{1}{2}\sqrt{\binom{n}{p}} \right\rfloor$ and reach higher values than those of most existing functions. In addition, the p-weight nonlinearity of h_4 is the highest when $p = 6, 7, 8, 9, 10$.

Table 2. The p-weight nonlinearity of known eight-variable WPB functions.

Functions	[7]	[8]	[9]	[11]	[10]	g_3 in [13]	h_3 in (10)	Upper Bound
NL_2	≤9	2	2	2	2	6	6	11
NL_3	≤22	12	14	12	12	8	17	24
NL_4	≤27	19	19	19	19	26	23	30
NL_5	≤22	12	14	12	12	8	17	24
NL_6	≤9	2	2	2	6	6	6	11

Table 3. The p-weight nonlinearity of known 16-variable WPB functions.

Function	NL_2	NL_3	NL_4	NL_5	NL_6	NL_7	NL_8	NL_9	NL_{10}	NL_{11}	NL_{12}	NL_{13}	NL_{14}
[8]	4	56	350	1312	3176	4782	5443	4782	3176	1312	350	56	4
[9]	4	112	686	1806	3436	4994	5603	4994	3436	1806	686	112	4
[11]	4	56	350	1288	3108	4774	5539	4902	3236	1672	654	152	28
[10]	4	56	350	1288	3108	4774	5539	4902	3228	1664	638	152	12
h_4 in (10)	12	104	590	1765	3487	5154	5827	5154	3491	1765	590	104	12
upper bound	54	268	888	2150	3959	5666	6378	5666	3959	2150	888	268	54

In the end, the algebraic immunities of the function h_m in (10) for $m = 2, 3, 4$ are given in Table 4. Their algebraic immunrere is relatively poor when m takes the value 4. Therefore, we still need to make more efforts on the WPB function for the optimal algebraic immunity with high weightwise nonlinearity.

Table 4. The algebraic immunity of h_m defined in (10), $m = 2, 3, 4$.

m	$AI(h_m)$	Optimal Algebraic Immunity
2	$AI(h_2) = 2$	2
3	$AI(h_3) = 3$	4
4	$AI(h_4) = 3$	8

5. Conclusions

In this paper, we gave a class of new 2^m-variable WPB functions and discussed the cryptographic properties of the new constructed WPB functions. We proved that their algebraic degree is $2^m - 1$. The experimental results demonstrated that some of the p-weight nonlinearity of this class of WPB functions is higher than any currently known WPB functions for small m. Although the state-of-the-art studies regarding WPB functions show that the p-weight nonlinearity is difficult to prove theoretically, we still need to conduct more research to obtain the p-weight nonlinearity for large m in the future. In addition, while Boolean functions motivated by FLIP have attracted the attention of many researchers in recent years, there is little research on filter functions of b-FLIP (b instances of FLIP in parallel), which is also a direction worthy of study.

Author Contributions: Conceptualization, Q.Z., Y.J., D.Z. and B.Q.; Investigation, Q.Z., Y.J., D.Z. and B.Q.; software, Q.Z. and Y.J.; Funding acquisition, Q.Z. and D.Z.; writing—original draft preparation, Q.Z. and Y.J.; writing—review and editing, Q.Z., Y.J., D.Z. and B.Q. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (Grant Nos. 61902314 and 62072371) and the Basic Research Program of Qinghai Province (Grant No. 2020-ZJ-701).

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Gentry, C. Fully homomorphic encryption using ideal lattices. In Proceedings of the 41st Annual ACM Symposium on Theory of Computing, Bethesda, MD, USA, 31 May–2 June 2009; pp. 169–178.
2. Méaux, P.; Journault, A.; Standaert, F.-X.; Carlet, C. Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts. *IACR Cryptol. ePrint Arch.* **2016**, *9665*, 311–343.
3. Filmus, Y. Friedgut-Kalai-Naor theorem for slices of the Boolean cube. *Chic. J. Theor. Comput. Sci.* **2016**, *14*, 1–17.
4. Filmus, Y. An orthogonal basis for functions over a slice of the Boolean hypercube. *Electron. J. Comb.* **2016**, *23*, 1–23. [CrossRef] [PubMed]
5. Duval, S.; Lallemand, V.; Rotella, Y. Cryptanalysis of the FLIP Family of Stream Ciphers. *IACR Cryptol. ePrint Arch.* **2016**, *9814*, 457–475.
6. 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. [CrossRef]
7. Liu, J.; Mesnager, S. Weightwise perfectly balanced functions with high weightwise nonlinearity profile. *Des. Codes Cryptogr.* **2019**, *87*, 1797–1813. [CrossRef]
8. Li, J.; Su, S. Construction of weightwise perfectly balanced Boolean functions with high weightwise nonlinearity. *Discrete Appl. Math.* **2020**, *279*, 218–227. [CrossRef]
9. Mesnager, S.; Su, S. On constructions of weightwise perfectly balanced functions. *Cryptogr. Commun.* **2021**, *13*, 951–979. [CrossRef]
10. Zhang, R.; Su, S. A new construction of weightwise perfectly balanced Boolean functions. *Adv. Math. Commun.* **2021**, *accepted*. [CrossRef]
11. Su, S. The lower bound of the weightwise nonlinearity profile of a class of weightwise perfectly balanced functions. *Discrete Appl. Math.* **2021**, *297*, 60–70. [CrossRef]
12. Tang, D.; Liu, J. A family of weightwise (almost) perfectly balanced boolean functions with optimal algebraic immunity. *Cryptogr. Commun.* **2019**, *11*, 1185–1197. [CrossRef]
13. Mesnager, S.; Su, S.; Li, J.; Zhu, L. Concrete constructions of weightwise perfectly balanced (2-rotation symmetric) functions with optimal algebraic immunity and high weightwise nonlinearity. *Cryptogr. Commun.* **2022**, *14*, 1371–1389. [CrossRef]
14. Richard, A. Orthogonal polynomials and special functions. In *Regional Conference Series in Applied Mathematics*; SIAM: Philadelphia, PA, USA, 1975.