A Class of Weightwise Almost Perfectly Balanced Boolean Functions with High Weightwise Nonlinearity

Deepak Kumar Dalai[1] and Krishna Mallick[2]
[1]School of Mathematical Sciences,
[2]School of Computer Sciences,
National Institute of Science Education and Research,
An OCC of Homi Bhabha National Institute,
Bhubaneswar, Odisha 752050, India
Email: {deepak, krishna.mallick}@niser.ac.in

Abstract

A Boolean function with good cryptographic properties over a set of vectors with constant Hamming weight is significant for stream ciphers like FLIP [MJSC16]. This paper presents a construction for weightwise almost perfectly balanced (WAPB) Boolean functions with good nonlinearity and good weightwise nonlinearities. We have presented the comparison of nonlinearity and weightwise nonlinearities with other available WAPB Boolean functions, which shows that this class of WAPB functions has the highest nonlinearities.

Keywords— Boolean function, FLIP cipher, Weightwise perfectly balanced (WPB), Weightwise almost perfectly balanced (WAPB)

1 Introduction

An n-variable Boolean function f is a mapping from the n-dimensional vector space $\mathbb{F}_2^n$ to $\mathbb{F}_2$, where $\mathbb{F}_2$ is a finite field with two elements $\{0, 1\}$. Depending upon the underlying algebraic structure, the '+' symbol is used for the addition operation in both $\mathbb{F}_2$ and $\mathbb{R}$. In stream ciphers, Boolean functions are used as a filter function for generating pseudorandom sequences; in some block ciphers, these functions are used to generate round keys. In these classical ciphers, the inputs to the function reach the whole space $\mathbb{F}_2^n$, whereas for reducing multiplicative depth in lightweight ciphers, the inputs can be restricted to some subsets of $\mathbb{F}_2^n$. The inputs to the filter function that has been used in the FLIP cipher introduced in [MJSC16] are restricted to the vectors of Hamming weight $\frac{n}{2}$. The analysis of different cryptographic criteria of Boolean functions over restricted domains arises after the work of Carlet, Méaux, and Rotella in [CMR17]. Therefore to avoid the biased output, one of the important cryptographic criteria for a Boolean function is balancedness over the defined domain. Moreover, it is desirable to construct Boolean functions over the set of vectors $E_{n,k} = \{x \in \mathbb{F}_2^n : w_H(x) = k\}$ for $1 \leq k \leq n-1$ with good cryptographic properties to avoid attacks. In [CMR17], Carlet et. al introduced the concepts of weightwise perfectly balanced (WPB) and weightwise almost perfectly balanced (WAPB) functions, which are balanced over $E_{n,k}$ for all k and its cryptographic criteria like nonlinearity and algebraic immunity over $E_{n,k}$.
There are several proposed methods for constructing WAPB and WPB (see [DLR16, CMR17, LM19, MZD19, TL19, LS20, MS21, MSL21, GM22, GS22, ZS22, ZS23, DM23]) in which the nonlinearity over $E_{n,k}$ of the defined functions have been discussed. Still, there is a noticeable gap in the upper bound of nonlinearity proposed in [CMR17] over $E_{n,k}$ (i.e., weightwise nonlinearity) and the known constructions. In our construction, we have attempted to reduce the gap in weightwise nonlinearity and also nonlinearity over $\mathbb{F}_2^n$.

2 Preliminaries

Let $\mathcal{B}_n$ be the set of all n-variable Boolean functions. Let us denote $[i,j]=\{i,i+1,\ldots,j\}$ for two integers i,j with $i\le j$. For any $v=(v_1,v_2,\ldots,v_n)\in\mathbb{F}_2^n$, the Hamming weight of v is defined as $\mathtt{wt}(v)=|\{i\in[1,n]:v_i=1\}|$. The support of a Boolean function $f\in\mathcal{B}_n$ is $\mathtt{sup}(f)=\{v\in\mathbb{F}_2^n:f(v)=1\}$ and Hamming weight of f is $\mathtt{wt}(f)=|\mathtt{sup}(f)|$. Let us denote $E_{n,k}=\{v\in\mathbb{F}_2^n:\mathtt{wt}(v)=k\}$ for every $k\in[0,n]$. The support and Hamming weight of f restricted to $E_{n,k}$ are denoted as $\mathtt{sup}_k(f)=\{v\in E_{n,k}:f(v)=1\}$ and $\mathtt{wt}_k(f)=|\mathtt{sup}_k(f)|$ respectively. The Hamming distance between two functions $f,g\in\mathcal{B}_n$ is given as $\mathtt{d}(f,g)=|\{v\in\mathbb{F}_2^n:f(v)\neq g(v)\}|=\mathtt{wt}(f+g)$ and the Hamming distance between two functions f,g restricted to $E_{n,k}$ is given as $\mathtt{d}_k(f,g)=|\{v\in E_{n,k}:f(v)\neq g(v)\}|=\mathtt{wt}_k(f+g)$. The truth table representation of a Boolean function $f\in\mathcal{B}_n$ is a 2^n-dimensional vector representation, i.e., $f=\{f(0,0,\ldots,0),f(0,0,\ldots,1),\ldots,f(1,1,\ldots,1)\}$. The algebraic normal form (ANF) representation is defined as $f(x)=\sum_{u\in\mathbb{F}_2^n}a_ux^u$, where $a_u\in\mathbb{F}_2$ and $x^u=x_1^{u_1}x_2^{u_2}\cdots x_n^{u_n}$ for $x=(x_1,x_2,\ldots,x_n)$. The algebraic degree of the Boolean function $f\in\mathcal{B}_n$ is defined as $\deg(f)=\max\{\mathtt{wt}(u):u\in\mathbb{F}_2^n,a_u\neq 0\}$. Any $f\in\mathcal{B}_n$, with $\deg(f)\le 1$, is said to be an affine Boolean function, and the set of all affine Boolean functions in $\mathcal{B}_n$ is denoted by $\mathcal{A}_n$. A Boolean function $f\in\mathcal{B}_n$ is balanced, if $\mathtt{wt}(f)=2^{n-1}$. The nonlinearity of $f\in\mathcal{B}_n$, denoted as $\mathtt{nl}(f)$, is the minimum Hamming distance of f to any affine function. That is, $\mathtt{nl}(f)=\min_{g\in\mathcal{A}_n}\mathtt{d}(f,g)$. Similarly, all these cryptographic criteria are also defined for the n-variable Boolean function when the inputs are restricted to $E_{n,k}$.

Definition 2.1. *[CMR17] A Boolean function $f\in\mathcal{B}_n$ is said to be weightwise almost perfectly balanced (WAPB) if, for every $k\in[0,n]$, $\mathtt{wt}_k(f)=\frac{\binom{n}{k}}{2}$ if $\binom{n}{k}$ is even and $\mathtt{wt}_k(f)=\frac{\binom{n}{k}\pm 1}{2}$ if $\binom{n}{k}$ is odd.*

Definition 2.2. *[CMR17] A Boolean function $f\in\mathcal{B}_n$ is said to be weightwise perfectly balanced (WPB) if the restriction of f to $E_{n,k}$, is balanced for all $k\in[1,n-1]$, i.e., $\binom{n}{k}$ is even and $\mathtt{wt}_k(f)=\frac{\binom{n}{k}}{2}$.*

Therefore, a WPB function $f_n\in\mathcal{B}_n$ exists if $n=2^m$ and a WAPB function $f\in\mathcal{B}_n$ is called WPB Boolean function for $n=2^m$ for a nonnegative integer m. A WPB Boolean function $f\in\mathcal{B}_n$ is balanced, if $f(0,0,\ldots,0)\neq f(1,1,\ldots,1)$. Hence, there are $2\prod_{k=1}^{n-1}\binom{\binom{n}{k}}{\binom{n}{k}/2}$ balanced WPB Boolean functions.

Definition 2.3. *[CMR17] The nonlinearity of $f\in\mathcal{B}_n$ over $E_{n,k}$, denoted as $\mathtt{nl}_k(f)$, is the Hamming distance of f to the set of all affine functions $\mathcal{A}_n$ when evaluated over $E_{n,k}$. That is, $\mathtt{nl}_k(f)=\min_{g\in\mathcal{A}_n}d_k(f,g)=\min_{g\in\mathcal{A}_n}\mathtt{wt}_k(f+g)$.*

Let $\triangle$ be the symbol represents the symmetric difference between two sets.

Proposition 2.4. *[MS21] For a positive integer $n=2^m$, let $f_n\in\mathcal{B}_n$ with support*

$$\mathtt{sup}(f_n)=\begin{cases}\{(x,1)\in\mathbb{F}_2^2:x\in\mathbb{F}_2\}=\{(0,1),(1,1)\} & \text{if } n=2,\\ \{(x,y):x,y\in\mathbb{F}_2^{\frac{n}{2}},\mathtt{wt}(x)\text{ is odd}\}\triangle\{(z,z):z\in\mathtt{sup}(f_{\frac{n}{2}})\} & \text{if } n>2.\end{cases}$$

Then f_n is a WPB Boolean function.

Proposition 2.5. *[DM23] For $n\ge 2$, let $f_n\in\mathcal{B}_n$ with support*

$$\mathtt{sup}(f_n)=\begin{cases}\{(x,1)\in\mathbb{F}_2^2:x\in\mathbb{F}_2\}=\{(0,1),(1,1)\} & \text{if } n=2,\\ \{(x,0)\in\mathbb{F}_2^n:x\in\mathtt{sup}(f_{n-1})\}\cup\{(x,1)\in\mathbb{F}_2^n:x\notin\mathtt{sup}(f_{n-1})\} & \text{if } n>2 \text{ and odd},\\ \{(x,y)\in\mathbb{F}_2^n:x,y\in\mathbb{F}_2^{\frac{n}{2}},\mathtt{wt}(x)\text{ is odd}\}\triangle\{(z,z)\in\mathbb{F}_2^n:z\in\mathtt{sup}(f_{\frac{n}{2}})\}, & \text{if } n>2 \text{ and even}.\end{cases}$$

Then f_n is a WAPB Boolean function.

The construction proposed in Proposition 2.5 is a generalization of the construction proposed in Proposition 2.4 to get a WAPB Boolean function. The construction proposed in Proposition 2.5 is important for our study as we will provide a construction that improves its nonlinearity.

Theorem 2.6. *[DM23] Let $f_n \in \mathcal{B}_n$ $(n > 2)$, defined as in Proposition 2.5. Then $\mathtt{nl}(f_n) = 2\mathtt{nl}(f_{n-1})$ if n is odd and $\mathtt{nl}(f_n) \le \mathtt{wt}(f_{\frac{n}{2}})$ if n is even.*

For n even, the nonlinearity of f_n is very low as $X_1 = \{(x,y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \text{ is odd}\}$ is the support of a linear function $\sum_{i=1}^{\frac{n}{2}} x_i$ and the cardinality of $X_2 = \{(z,z) \in \mathbb{F}_2^n : z \in \mathtt{sup}(f_{\frac{n}{2}})\}$ is $\mathtt{wt}(f_{\frac{n}{2}})$. Further, for n even and k odd, $\mathtt{sup}_k(f_n) = \mathtt{sup}(f_n) \cap E_{n,k} = \{(x,y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \text{ is odd}\} \cap E_{n,k} = \mathtt{sup}_k(\sum_{i=1}^{\frac{n}{2}} x_i)$ and hence $\mathtt{nl}_k(f_n) = 0$. Therefore, in our technique, we attempt to permute the coordinates of the vectors of weight k in X_1 to improve the nonlinearity by avoiding the linear patterns and preserving the weightwise balancedness.

3 A class of WAPB Boolean functions with good nonlinearity

In this case, $\mathtt{nl}_k(f_n) = 0$ as described above. Here, we will present a class of WAPB Boolean functions by modifying $\mathtt{sup}(f_n)$ presented in Proposition 2.5. We observed that the nonlinearity becomes weak because the $\mathtt{sup}(f_n)$ when n is even is close to a linear function. In our technique, we attempt to increase the nonlinearity by permuting the coordinates of some vectors in $\mathtt{sup}(f_n)$ when n is even.

Therefore, it is assumed that $n > 2$ and is **even** in this section. Hence, when n is even, as Proposition 2.5, $\mathtt{sup}(f_n) = \{(x,y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \text{ is odd}\} \triangle \{(z,z) \in \mathbb{F}_2^n : z \in \mathtt{sup}(f_{\frac{n}{2}})\}$. Then

$$\mathtt{sup}_k(f_n) = \begin{cases} \{(x,y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \text{ is odd}, \mathtt{wt}(x) + \mathtt{wt}(y) = k\} & \\ \qquad \triangle \{(z,z) \in \mathbb{F}_2^n : z \in \mathtt{sup}_{\frac{k}{2}}(f_{\frac{n}{2}})\} & \text{if } k \text{ is even} \\ \{(x,y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \text{ is odd}, \mathtt{wt}(x) + \mathtt{wt}(y) = k\} & \text{if } k \text{ is odd} \end{cases}$$

Now we will consider both cases of k (i.e., odd or even) and will propose to permute the coordinates of some vectors in $\mathtt{sup}_k(f_n)$.

3.1 When k is odd

In this case, $\mathtt{sup}_k(f_n) = \{(x,y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \text{ is odd}, \mathtt{wt}(x) + \mathtt{wt}(y) = k\} = \mathtt{sup}_k(\sum_{i=1}^{\frac{n}{2}} x_i)$ as we discussed at the end of Section 2. The linear function $l = \sum_{i=1}^{\frac{n}{2}} x_i$ is independent of y. We attempt to break the independence and linearity on the cordinates in y using the support of a nonlinear function $a \in \mathcal{B}_{\frac{n}{2}}$. That is, for every $x \in \mathbb{F}_2^{\frac{n}{2}}$ satisfying l (i.e., $\mathtt{wt}(x)$ is odd), we keep (x,y) if $y \in \sup(a)$ otherwise we replace (x,y) by (y,x). If a is a highly nonlinear function, then the component y is expected to be far from the linear functions and results a high nonlinearity in f.

Here, if $\mathtt{wt}((x,y)) = k$ then $\mathtt{wt}((y,x)) = k$. Further, if $(x,y) \in \sup_k(f_n)$ then $\mathtt{wt}(y)$ is even as $\mathtt{wt}(x)$ is odd. So, $(y,x) \notin \sup_k(f_n)$ if $(x,y) \in \sup_k(f_n)$. Therefore, replacement of $(x,y) \in \sup_k(f_n)$ by (y,x) does not change the weight of the resultant function in the domain $E_{n,k}$.

Lemma 3.1. *Let $a \in \mathcal{B}_{\frac{n}{2}}$. A function $f \in \mathcal{B}_n$ such that for every $k \in [0,n]$ and odd,*

$$\begin{aligned} \mathtt{sup}_k(f^a) \quad = \quad & \{(x,y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \text{ is odd}, y \in \mathtt{sup}(a), \mathtt{wt}(y) = k - \mathtt{wt}(x)\} \\ & \cup \{(y,x) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \text{ is odd}, y \notin \mathtt{sup}(a), \mathtt{wt}(y) = k - \mathtt{wt}(x)\}. \end{aligned} \tag{1}$$

Then $\mathtt{wt}_k(f^a) = \frac{1}{2}\binom{n}{k}$.

3.2 When k is even

In this case, $\mathtt{sup}_k(f_n) = \{(x,y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \text{ is odd}, \mathtt{wt}(x) + \mathtt{wt}(y) = k\} \triangle \{(z,z) \in \mathbb{F}_2^n : z \in \mathtt{sup}_{\frac{k}{2}}(f_{\frac{n}{2}})\}$. Let us denote the set $L = \{(x,y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \text{ is odd}, \mathtt{wt}(x) + \mathtt{wt}(y) = k\}$ and $M = \{(z,z) \in \mathbb{F}_2^n : z \in \mathtt{sup}_{\frac{k}{2}}(f_{\frac{n}{2}})\}$. In this case, the replacement of $(x,y) \in \sup_k(f_n)$ by (y,x) is not straight forward as in Subsection 3.1. If $(x, y) \in L$ then $\mathtt{wt}(y)$ is odd as $\mathtt{wt}(x)$ is odd. As a result, (y, x) could be present in L. Therefore, replacement of $(x, y) \in \sup_k(f_n)$ by (y, x) can possibly duplicate an existing vector in L, which reduces the weight of the resultant function. Therefore, we attempt to swap two bits x_i and y_i in stead of swapping x and y as in the following lemma. For given $(x, y) \in \mathbb{F}_2^n$ where $x = (x_1, \ldots, x_{\frac{n}{2}}), y = (y_1, \ldots, y_{\frac{n}{2}}) \in \mathbb{F}_2^{\frac{n}{2}}$, denote $(x^i, y^i) = (x_1, \ldots, x_{i-1}, y_i, x_{i+1}, \ldots, x_{\frac{n}{2}}, y_1, \ldots, y_{i-1}, x_i, y_{i+1}, \ldots, y_{\frac{n}{2}})$. That is, (x^i, y^i) is obtained by swapping the i-th bits of x and y.

Lemma 3.2. *Let $f_n \in \mathcal{B}_n$ be the function defined in Proposition 2.5. For every $k \in [0, n]$ and even, let $W_k = \{(x, y) \in \mathtt{sup}_k(f_n) | \mathtt{wt}(x)$ is odd, and there is an $i \in [1, \frac{n}{2}]$ such that $x_j = y_j$ for $1 \leq j \leq i - 1$ and $y_i = 1, x_i = 0\}$ and*
$W'_k = \{(x^i, y^i) | (x, y) \in W_k$ and $i \in [1, \frac{n}{2}]$ such that $x_j = y_j$ for $1 \leq j \leq i-1$ and $y_i = 1, x_i = 0$ i.e., the i obtained for(x, y) in $W_k\}$.
A function $g_n \in \mathcal{B}_n$ such that $\mathtt{sup}_k(g_n) = (\mathtt{sup}_k(f_n) \setminus W_k) \cup W'_k$ for every $k \in [0, n]$ and even.
Then $\mathtt{wt}_k(g_n) = \mathtt{wt}_k(f_n)$ if k is even.

Like in Lemma 3.1, now we will use the support of another Boolean function (possibly, a highly nonlinear) to swap x^i and y^i in some of $(x^i, y^i) \in W'_k$ as defined in Lemma 3.2.

Lemma 3.3. *Let $b \in \mathcal{B}_{\frac{n}{2}}$. Let $g_n \in \mathcal{B}_n$ as defined in Lemma 3.2 with W_k and W'_k. A function $h_n^b \in \mathcal{B}_n$ such that for every $k \in [0, n]$ and even,*
$\mathtt{sup}_k(h_n^b) = \{(x, y) \in \mathtt{sup}_k(g_n) : (x, y) \notin W'_k\} \cup \{(x, y) : (x, y) \in W'_k$ and $y \in \mathtt{sup}(b)\} \cup \{(y, x) : (x, y) \in W'_k$ and $y \notin \mathtt{sup}(b)\}$.
Then $\mathtt{wt}_k(h_n^b) = \mathtt{wt}_k(g_n)$.

3.3 A class of WAPB Boolean functions

Now we will apply Lemma 3.1 and Lemma 3.3 to construct a WAPB Boolean function with improved nonlinearity.

Theorem 3.4. *Let $a, b \in \mathcal{B}_{\frac{n}{2}}$. Let $f_n \in \mathcal{B}_n$ be the function defined in Proposition 2.5. Let $F_n \in \mathcal{B}_n$ with support $\mathtt{sup}_k(F_n) = \begin{cases} \mathtt{sup}_k(h_n^b) & \text{if } k \text{ is even} \\ \mathtt{sup}_k(f_n^a) & \text{if } k \text{ is odd,} \end{cases}$*
where f_n^a, h_n^b are as defined in Lemma 3.1 and Lemma 3.3 respectively. Then F_n is a WAPB Boolean function.

The following is a recursive construction of a WAPB Boolean function.

Construction 3.5. *For $n \geq 2$, let $F_n \in \mathcal{B}_n$ with support*

$$\mathtt{sup}(F_n) = \begin{cases} \{(x, 1) \in \mathbb{F}_2^2 : x \in \mathbb{F}_2\} = \{(0, 1), (1, 1)\} & \text{if } n = 2, \\ \{(x, 0) \in \mathbb{F}_2^n : x \in \mathtt{sup}(F_{n-1})\} \cup \{(x, 1) \in \mathbb{F}_2^n : x \notin \mathtt{sup}(F_{n-1})\} & \text{if } n > 2 \text{ and odd,} \\ S_n \triangle \{(z, z) \in \mathbb{F}_2^n : z \in \mathtt{sup}(F_{\frac{n}{2}})\} & \text{if } n > 2 \text{ and even.} \end{cases}$$

Here $S_n = \cup_{k=0}^n \mathtt{sup}_k(F_n)$ and $\mathtt{sup}_k(F_n) = \begin{cases} \mathtt{sup}_k(h_n^b) & \text{if } n > 2 \text{ and even and } k \text{ is even} \\ \mathtt{sup}_k(h_n^a) & \text{if } n > 2 \text{ and even and } k \text{ is odd.} \end{cases}$

3.4 Experimental results on nonlinearity

In this section, we have presented experimental results on the nonlinearity ($\mathtt{nl}(F_n)$) and weightwise nonlinearity ($\mathtt{nl}_k(F_n)$) of F_n. We have chosen $a, b \in \mathcal{B}_{\frac{n}{2}}$, a highly nonlinear function

$$a(y) = b(y) = \begin{cases} y_1 y_2 + \cdots + y_{\frac{n}{2}-1} y_{\frac{n}{2}} & \text{if } \frac{n}{2} \text{ is even} \\ y_1 y_2 + \cdots + y_{\frac{n}{2}-2} y_{\frac{n}{2}-1} + y_{\frac{n}{2}} & \text{if } \frac{n}{2} \text{ is odd.} \end{cases}$$

This function is a bent function when n is even and concatenation of two bent functions when n is odd. Further, these two functions are easy to compute which is helpful for implementation in light weight

n	nl	$\texttt{nl}_2$	$\texttt{nl}_3$	$\texttt{nl}_4$	$\texttt{nl}_5$	$\texttt{nl}_6$	$\texttt{nl}_7$	$\texttt{nl}_8$	$\texttt{nl}_9$	$\texttt{nl}_{10}$	$\texttt{nl}_{11}$	$\texttt{nl}_{12}$	$\texttt{nl}_{13}$	$\texttt{nl}_{14}$	$\sum_{k=0}^{n} \texttt{nl}_k$
8	96	4	16	20	16	4	0	0	-	-	-	-	-	-	60
9	192	6	22	45	45	22	6	0	0	-	-	-	-	-	146
10	416	9	36	69	94	73	12	9	0	0	-	-	-	-	302
11	832	11	50	113	163	173	117	34	11	0	0	-	-	-	672
12	1596	12	36	146	264	286	264	148	36	14	0	0	-	-	1206
13	3192	15	69	219	507	660	660	495	240	69	17	0	0	-	2951
14	6904	19	102	336	764	1083	1484	1079	654	299	30	18	0	0	5868
15	13808	22	147	474	1155	2013	2735	2670	1965	1154	465	75	22	0	12897
16	28152	24	64	564	1216	2547	5036	4610	5036	2919	1216	516	64	24	23836

Table 1: Listing of $\texttt{nl}(F_n), \texttt{nl}_k(F_n)$ and $\sum_{k=0}^{n} \texttt{nl}_k(F_n)$ for $8 \leq n \leq 16$.

cryptography. Table 1 presents the nonlinearity and weightwise nonlinearity of the functions F_n for $n = 8, 9, \ldots, 16$, which are generated using Construction 3.5.

We have presented a comparison of weightwise nonlinearities of F_n with the upper bound presented in [CMR17] in Table 2. Further, no upper bound is available for the nonlinearity of WAPB Boolean functions. Therefore, we have presented a comparison of the nonlinearity of F_n with the upper bound of the nonlinearity of n variable Boolean functions [dH97].

n	*function*	nl	$\texttt{nl}_2$	$\texttt{nl}_3$	$\texttt{nl}_4$	$\texttt{nl}_5$	$\texttt{nl}_6$	$\texttt{nl}_7$	$\texttt{nl}_8$	$\texttt{nl}_9$	$\texttt{nl}_{10}$	$\texttt{nl}_{11}$	$\sum_{k=0}^{n} \texttt{nl}_k$
8	*UB*	120	11	24	30	24	11	-	-	-	-	-	100
	F_8	96	4	16	20	16	4	-	-	-	-	-	60
9	*UB*	244	15	37	57	57	37	15	-	-	-	-	218
	F_9	192	6	22	45	45	22	6	-	-	-	-	146
10	*UB*	496	19	54	97	118	97	54	19	-	-	-	498
	F_{10}	416	9	36	69	94	73	12	9	-	-	-	302
11	*UB*	1000	23	76	155	220	220	155	76	23	-	-	948
	F_{11}	832	11	50	113	163	173	117	34	11	-	-	672
12	*UB*	2016	28	102	236	381	446	381	236	102	28	-	1940
	F_{12}	1596	12	36	146	264	286	264	148	36	14	-	1206
13	*UB*	4050	34	134	344	625	837	837	625	344	134	34	3948
	F_{13}	3192	15	69	219	507	660	660	495	240	69	17	2951

Table 2: Comparison of $\texttt{nl}_k(F_n)$ with the upper bound(UB) presented in [CMR17]

We compare the nonlinearities of our result with some recent constructions for $n = 8$ in Table 3. The sum of the weightwise nonlinearity of our construction is highest for $n = 8$ among the available constructions.

4 Conclusions and Future work

We have presented constructing a class of WAPB Boolean functions in n variables from the idea of constructions presented in [MS21, DM23]. The experimental results on nonlinearity and weightwise nonlinearities show a good improvement and are the highest among the available constructions. For future work, we are studying the cryptographic properties of this class of WAPB functions and attempting to further improve the nonlinearities and weightwise nonlinearities by modifying this class of functions.

WPB/ WAPB functions	$\mathtt{nl}_2$	$\mathtt{nl}_3$	$\mathtt{nl}_4$	$\mathtt{nl}_5$	$\mathtt{nl}_6$	$\sum_{k=0}^{8}\mathtt{nl}_k$
Upper Bound [CMR17]	11	24	30	24	11	100
Carlet, Méaux, Rotella [CMR17]	2	12	19	12	2	47
Li and Su [LS20, g_{2^q+2} Equation(9)]	2	12	19	12	2	47
Mesnager and Su [MS21, f_m Equation(13)]	2	0	3	0	2	7
Mesnager and Su [MS21, g_m Equation(22)]	2	14	19	14	2	51
Mesnager, Su and Li [MSL21, f_m Equation(2)]	2	8	8	8	2	28
Mesnager, Su and Li [MSL21, f_m Equation(3)]	6	8	26	8	6	54
Zhang and Su [ZS23, g_m Equation(11)]	2	12	19	12	6	51
F_n[Construction 3.5]	4	16	20	16	4	60

Table 3: Comparison of $\mathtt{nl}_k$ of 8-variable WPB constructions.

References

[CMR17] Claude Carlet, Pierrick Méaux, and Yann Rotella. Boolean functions with restricted input and their robustness; application to the FLIP cipher. *IACR Trans. Symmetric Cryptol.*, 2017(3):192–227, 2017.

[dH97] Xiang dong Hou. On the norm and covering radius of the first-order Reed-Muller codes. *IEEE Transactions on Information Theory*, 43(3):1025–1027, 1997.

[DLR16] Sébastien Duval, Virginie Lallemand, and Yann Rotella. Cryptanalysis of the FLIP family of stream ciphers. In *Advances in Cryptology - CRYPTO 2016*, volume 9814 of *Lecture Notes in Computer Science*, pages 457–475. Springer, 2016.

[DM23] Deepak Kumar Dalai and Krishna Mallick. A class of weightwise almost perfectly balanced boolean functions. In *ALgebraic and combinatorial methods for COding and CRYPTography-ALCOCRYPT*, 2023.

[GM22] Agnese Gini and Pierrick Méaux. On the weightwise nonlinearity of weightwise perfectly balanced functions. *Discrete Applied Mathematics*, 322:320–341, 2022.

[GS22] Xiaoqi Guo and Sihong Su. Construction of weightwise almost perfectly balanced boolean functions on an arbitrary number of variables. *Discrete Applied Mathematics*, 307:102–114, 2022.

[LM19] Jian Liu and Sihem Mesnager. Weightwise perfectly balanced functions with high weightwise nonlinearity profile. *Designs, Codes and Cryptography*, 87(8):1797–1813, 2019.

[LS20] Jingjing Li and Sihong Su. Construction of weightwise perfectly balanced boolean functions with high weightwise nonlinearity. *Discrete Applied Mathematics*, 279:218–227, 2020.

[MJSC16] Pierrick Méaux, Anthony Journault, François-Xavier Standaert, and Claude Carlet. Towards stream ciphers for efficient FHE with low-noise ciphertexts. In *Advances in Cryptology - EUROCRYPT 2016*, volume 9665 of *Lecture Notes in Computer Science*, pages 311–343. Springer, 2016.

[MS21] Sihem Mesnager and Sihong Su. On constructions of weightwise perfectly balanced boolean functions. *Cryptography and Communications*, 13(6):951–979, 2021.

[MSL21] Sihem Mesnager, Sihong Su, and Jingjing Li. On concrete constructions of weightwise perfectly balanced functions with optimal algebraic immunity and high weightwise nonlinearity. In *The 6th International Workshop on Boolean Functions and Applications*, 2021.

[MZD19] Sihem Mesnager, Zhengchun Zhou, and Cunsheng Ding. On the nonlinearity of boolean functions with restricted input. *Cryptography and Communications*, 11(1):63–76, 2019.

[TL19] Deng Tang and Jian Liu. A family of weightwise (almost) perfectly balanced boolean functions with optimal algebraic immunity. *Cryptography and Communications*, 11(6):1185–1197, 2019.

[ZS22] Linya Zhu and Sihong Su. A systematic method of constructing weightwise almost perfectly balanced boolean functions on an arbitrary number of variables. *Discrete Applied Mathematics*, 314:181–190, 2022.

[ZS23] Rui Zhang and Sihong Su. A new construction of weightwise perfectly balanced boolean functions. *Advances in Mathematics of Communications*, 17(4):757–770, 2023.