A Class of Weightwise Almost Perfectly Balanced Boolean Functions

Abstract

The construction of Boolean functions with good cryptographic properties over a subset of vectors with fixed Hamming weight $E_{n,k} \subset \mathbb{F}_2^n$ is significant in lightweight stream ciphers like FLIP [MJSC16]. In this article, we have given a construction for a class of n-variable weightwise almost perfectly balanced (WAPB) Boolean functions from known support of an n_0-variable WAPB where $n_0 < n$. This is a generalization of constructing a weightwise perfectly balanced (WPB) Boolean function by Mesnager and Su [MS21]. At the end of this article, we have also studied some cryptographic properties like ANF, weight, and nonlinearity of the functions. The ANF of this function is recursive, which would be a low-cost implementation in a lightweight stream cipher. The nonlinearity of this class of functions is very poor.

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 underlying algebraic structure, '+' symbol is used for the addition operation in both $\mathbb{F}_2$ and $\mathbb{R}$. The Boolean functions are used as a filter function in stream ciphers to generate a pseudo-random sequence. Some cryptographic criteria have been defined to analyze and construct Boolean functions for use in the ciphers to resist different attacks. Generally, the cryptographic criteria of a filter function are defined over the entire domain of vector space $\mathbb{F}_2^n$. The study of the Boolean functions over a restricted domain became interesting after the appearance of the stream cipher FLIP in 2016 [MJSC16]. The main idea of proposing the cipher FLIP is to combine the symmetric cipher with homomorphic encryption to achieve an admissible scheme for delegated computations through cloud services. In this new stream cipher design, the inputs are permuted by a bit permutation generator before entering the filter function in each updating processing. Therefore, the whole setup is known as a filter permutator. So, the Hamming weight (i.e., the number of non-zero coordinates) of the inputs to the filter function remains the same as the Hamming weight of the secret key. This restriction of the inputs significantly changes the viewpoint toward the security analysis of it. Cryptanalysis of the initial version of FLIP and some modifications in the filter function are presented in [DLR16]. However, the motivation to construct Boolean functions in the FLIP frame of reference arises. An initial cryptographic study of Boolean function in a restricted domain is introduced by Carlet et al. in [CMR17]. The mathematical introduction of the required parameters (i.e., balancedness, nonlinearity, and algebraic immunity) of a Boolean function in a restricted domain of $\mathbb{F}_2^n$ are presented in the paper.

Unlike the FLIP cipher, no prior relations are defined, in general, over the inputs of the Boolean function in the stream cipher. The Boolean functions used as filter functions in stream cipher are distributed uniformly over $\mathbb{F}_2^n$ and are called balanced Boolean functions. In this new model, the Hamming weight of the key register is known (i.e., $\frac{n}{2}$ for n even). Therefore, the keystream should look like a random sequence over the restricted domain (i.e., the set of vectors of the constant Hamming weight). So it is preferred to use a filter function by allowing a small bias in the keystream to hide the Hamming weight of the inputs over the set of vectors with constant weight. Therefore, the filter functions balanced over the subsets of $\mathbb{F}_2^n$ containing vectors with constant Hamming weight are said to be weightwise perfectly balanced (WPB). The functions with good cryptographic criteria over the restricted domains are essential in the FLIP frame of reference. Some critical cryptographic criteria of a Boolean function over a restricted domain are studied in [CMR17].

An upper bound on the nonlinearity of a Boolean function on restricted inputs is presented in [CMR17]. The nonlinearity bound is further improved in [MZD19]. In [MMM$^+$20]

The first weightwise perfectly balanced (WPB) Boolean function construction was introduced in [CMR17] in 2017. The construction is based on the direct sum of two WPB Boolean functions of 2^n- variable by modifying one of the WPB functions. A generalized result is presented by using four Boolean functions. The author also presented a recursive construction for weightwise almost perfectly balanced (WAPB) Boolean functions in the same paper. In [LM19], Jian Liu and Sihem Mesnager have presented a construction for a class of WPB Boolean functions of 2^n-variables. A subclass of their constructed WPB Boolean functions satisfies high weightwise nonlinearity. In 2020, Jingjing Li and Sihong Su in [LS20] provided a construction for a class of WAPB Boolean function of 2^{q+2}-variable for $q \geq 1$ and then constructed a WPB of variable 2^{q+2} by modifying the support of the WAPB Boolean function. Several constructions of WPB and WAPB Boolean functions are presented in [MS21] by modifying the support of linear and quadratic functions. Recently in 2022, some constructions for WAPB Boolean functions are presented in [ZS22, GS22].

1.1 Our Contributions

In this paper, we have given a construction for a class of WAPB Boolean functions on any arbitrary number of variables n. We also have discussed the nonlinearity of the constructed WAPB over $\mathbb{F}_2^n$. Then we try to improve the nonlinearity of the WAPB by changing the Boolean function that we use as initialized function in this recursive construction.

1.2 Organisation

The research objectives and our contributions are already outlined. The remaining part of the paper is organized as follows.

2 Preliminary

Let $\mathcal{B}_n$ be the set of all n-variable Boolean functions. Let denote $[i,j] = \{i, i+1, \dots, j\}$ for two integers i, j with $i \leq j$. For any $v = (v_1, v_2, \dots, v_n) \in \mathbb{F}_2^n$, 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 $\mathcal{E}_n$ be the family of subsets $E_{n,k} = \{v \in \mathbb{F}_2^n : \mathtt{wt}(v) = k\}$ for $k \in [0,n]$ of $\mathbb{F}_2^n$. The support and Hamming weight of f restricted to $E_{n,k}$ are denoted as $\mathtt{sup}_k(f_n) = \{v \in E_{n,k} : f(v) = 1\}$ and $\mathtt{wt}_k(f) = |\mathtt{sup}_k(f_n)|$ respectively. The Hamming distance between two functions $f, g \in \mathcal{B}_n$ is given as $\mathtt{d}(f,g) = |\{v \in \mathbb{F}_2^n : f(v) \neq g(v)\}| = \mathtt{wt}(f+g)$.

A basic representation of Boolean function (known as the truth table representation) is the 2^n-tuple vector representation i.e., $f = \{f(0,0,\dots,0), f(0,0,\dots,1), \dots, f(1,1,\dots,1)\}$. Another representation is algebraic normal form (ANF), which is a multi-variable polynomial over $\mathbb{F}_2$. The ANF of $f \in \mathcal{B}_n$ is defined as $f(x) = \sum_{u \in \mathbb{F}_2^n} a_u x^u$, where $a_u \in \mathbb{F}_2$ and $x^u = x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n}$ for $x = (x_1, x_2, \dots, x_n)$. 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 $\deg(f) \leq 1$ 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 Boolean function that is used for cryptographic algorithm should be balanced to look like a random sequence when the inputs goes through all the elements of $\mathbb{F}_2^n$. The nonlinearity of $f \in \mathcal{B}_n$, denoted as $\mathtt{nl}(f)$ is the Hamming distance of f from the set of all affine functions. 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 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 $\mathtt{wt}_k(f) = \frac{\binom{n}{k}}{2}$.*

Definition 2.2. *[CMR17] A Boolean function $f \in \mathcal{B}_n$ is said to be weightwise almost perfectly balanced*

(WAPB), if for all $k \in [0, n]$,

$$\mathtt{wt}_k(f) = \begin{cases} \frac{\binom{n}{k}}{2}, & \textit{if } \binom{n}{k} \textit{ is even,} \\ \frac{\binom{n}{k} \pm 1}{2}, & \textit{if } \binom{n}{k} \textit{ is } \quad \textit{odd.} \end{cases}$$

Let $x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots, y_n) \in \mathbb{F}_2^n$, then y covers x (i.e., $x \preceq y$), if $x_i \leq y_i \forall i \in [n]$. A remarkable theorem [Luc78] was presented by Érdouard Lucas in 1878 that provides a simple way to evaluate the binomial coefficient $\binom{n}{k}$ modulo a prime p. The same has been used to compute $\binom{n}{k}$ is odd or even.

Proposition 2.3 (Lucas Theorem)**.** *Let the binary representation of n and k be $(n_1, n_2, \dots, n_l)$ and $(k_1, k_2, \dots, k_l)$ respectively, where $n_i, k_i \in \{0, 1\}$ for $i \in [l]$, then*

$$\binom{n}{k} = \begin{cases} 1(mod\, 2) & if\, k \preceq n \\ 0(mod\, 2) & if\, k \npreceq n. \end{cases}$$

Hence, it is straightforward from Theorem 2.3 that $\binom{n}{k}$ is even for all $k \in [1, n-1]$ iff $n = 2^m$ for a nonnegative integer m. Then we have the following corollaries on the existence of the WPB functions.

Corollary 2.4. *[CMR17] If $f \in B_n$ is a WPB Boolean function then $n = 2^m$ for a nonnegative integer m.*

Corollary 2.5. *If $n = 2^m$ for a nonnegative integer m then there are $4 \prod_{k=1}^{n-1} \binom{\binom{n}{k}}{\binom{n}{k}/2}$ WPB Boolean functions on n variable.*

A WPB Boolean function $f \in \mathcal{B}_n$ is balanced, if $f(0, 0, \dots, 0) \neq f(1, 1, \dots, 1)$. Hence, there are $2 \prod_{k=1}^{n-1} \binom{\binom{n}{k}}{\binom{n}{k}/2}$ balanced WPB Boolean functions. Such kind of Boolean functions with good cryptographic criteria over $E_{n,k}$ are significant for the stream cipher FLIP. The nonlinearity of a Boolean function over a restricted domain is introduced in [CMR17].

Definition 2.6. *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, $\mathtt{nl}_k(f) = \min_{g \in \mathcal{A}_n} d_k(f, g) = \min_{g \in \mathcal{A}_n} \mathtt{wt}_k(f + g)$.*

The following identity and upper bound on nonlinearity of a Boolean function over $E_{n,k}$ can be derived. The upper bound is further improved by Mesnager et al in [MZD19].

Lemma 2.7. *[CMR17] If $f \in B_n$ then*

$$\mathtt{nl}_k(f) = \frac{|E_{n,k}|}{2} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |\sum_{x \in E_{n,k}} (-1)^{f(x) + a.x}| \textit{ and}$$

$$\mathtt{nl}_k(f) \leq \frac{1}{2}[|E_{n,k}| - \sqrt{|E_{n,k}|}]$$

for $k \in [0, n]$ (where $|E_{n,k}| = \binom{n}{k}$).

For crypographic use, specially in lightweight ciphers, the Boolean functions need to have good cryptographic properties along with simple algebraic normal form for fast computation, inexpensive implementation and energy efficiency. The first construction for the class of WPB and WAPB Boolean functions have been introduced by Carlet et al. in [CMR17] using the direct sum of Boolean functions. Let $f \in \mathcal{B}_n$ and $g \in \mathcal{B}_m$, then The direct sum of $f \in \mathcal{B}_n, g \in \mathcal{B}_m$ forms a Boolean function $h \in \mathcal{B}_{n+m}$ such that $h(x, y) = f(x) + g(y)$, *where* $x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^m$. The following propositions present some of the constructions of WPB and WAPB Boolean functions available in the literature.

Proposition 2.8. *[CMR17] Let $f, f', g, g' \in \mathcal{B}_n$ where f, f', g are WPB functions. Then the function $h \in \mathcal{B}_{2n}$ is defined by $h(x, y) = f(x) + \prod_{i=1}^{n} x_i + g(y) + (f(x) + f'(x))g'(y)$, where $x, y \in \mathbb{F}_2^n$, is a WPB Boolean function.*

Proposition 2.9. *[CMR17] Let $f_n \in \mathcal{B}_n$ for $n \geq 3$, be defined by*

$$f_n(x_1, x_2, \ldots, x_n) = \begin{cases} f_{n-1}(x_1, x_2, \ldots, x_{n-1}) & \textit{if } n \textit{ is } \quad \textit{odd} \text{ ,} \\ f_{n-1}(x_1, x_2, \ldots, x_{n-1}) + x_{n-2} + \displaystyle\prod_{i=1}^{2^{d-1}} x_{n-i} & \textit{if } n = 2^d; d > 1, \\ f_{n-1}(x_1, x_2, \ldots, x_{n-1}) + x_{n-2} + \displaystyle\prod_{i=1}^{2^{d}} x_{n-i} & \textit{if } n = p.2^d; p > 1 \textit{ odd}; d \geq 1. \end{cases}$$

where $f_2(x_1, x_2) = x_1$, is a WAPB Boolean function.

Proposition 2.10. *[MS21] For a positive integer $n = 2^m$, the support of $f_n \in \mathcal{B}_n$ is defined by*

$$\begin{aligned} \mathtt{sup}(f_n) &= \triangle_{i=1}^{m}\{(x, y, x, y, \ldots, x, y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{2^{m-i}}, \mathtt{wt}(x) \textit{ is odd}\}. \\ &= \begin{cases} \{(1, y) : y \in \mathbb{F}_2\} & \textit{if } n = 2, \\ \{(x, y) : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \textit{ is odd}\} \triangle \{(x, x) : x \in \mathtt{sup}(f_{\frac{n}{2}})\} & \textit{if } n > 2. \end{cases} \end{aligned}$$

Then the Boolean function f_n is WPB.

Corollary 2.11. *[MS21] The ANF of the Boolean function f_n proposed in Proposition 2.10 is*

$$f_n(x_1, x_2, \ldots, x_n) = \begin{cases} x_1 & \textit{if } n = 2, \\ \displaystyle\sum_{i=1}^{\frac{n}{2}} x_i + f_{\frac{n}{2}}(x_1, x_2, \ldots, x_{\frac{n}{2}}) + \prod_{i=1}^{\frac{n}{2}} (x_i + x_{\frac{n}{2}+i} + 1) & \textit{if } n > 2. \end{cases}$$

The construction proposed in Proposition 2.10 is important for our study as we will provide a construction which generalizes it. The following WAPB construction presented in [ZS22] is based on the direct sum of WPB Boolean functions of n_is variables where n_is are distinct powers of 2.

Proposition 2.12. *[ZS22] Let $n = n_1 + n_2 + \cdots + n_p$ for n_i being the power of 2 for $1 \leq i \leq p$ and $0 < n_1 < n_2 < \cdots < n_p$. Let $f_{n_i} \in \mathcal{B}_{n_i}$ be WPB with $f_{n_i}(0, 0, \ldots, 0) = 0, f_{n_i}(1, 1, \ldots, 1) = 1$ for $1 \leq i \leq p$. Then $h \in \mathcal{B}_n$ defined as*

$$h_n(x_1, x_2, \ldots, x_n) = f_{n_1}(x_1, x_2, \ldots, x_{n_1}) + f_{n_2}(x_{n_1+1}, x_{n_1+2}, \ldots, x_{n_1+n_2}) + \cdots + f_{n_p}(x_{n-n_p+1}, x_{n-n_p+2}, \ldots, x_n)$$

is WAPB.

The following combinatorial identities are useful for our study and construction. The book [Gou72] contains a list of very useful combinatorial identities and inequalities.

Lemma 2.13. *[Gou72, Item3.10] For the positive integers m, k, we have*

$$\sum_{i=0}^{\lfloor \frac{k-1}{2} \rfloor} \binom{m}{2i+1} \binom{m}{k-(2i+1)} = \frac{1}{2}\binom{2m}{k} + \frac{(-1)^{\frac{k}{2}}}{2} \binom{m}{\frac{k}{2}} \frac{1+(-1)^k}{2}.$$

1. *If k is odd, that implies* $\displaystyle\sum_{\substack{j=0 \\ j \textit{ is odd}}}^{k} \binom{m}{j}\binom{m}{k-j} = \frac{1}{2}\binom{2m}{k}.$

2. *If k is even, that implies* $\displaystyle\sum_{\substack{j=0 \\ j \textit{ is odd}}}^{k} \binom{m}{j}\binom{m}{k-j} = \frac{1}{2}\binom{2m}{k} - (-1)^{\frac{k}{2}}\binom{m}{\frac{k}{2}}.$

   (a) *If $\frac{k}{2}$ is odd, that implies* $\displaystyle\sum_{\substack{j=0 \\ j \textit{ is odd}}}^{k} \binom{m}{j}\binom{m}{k-j} = \frac{1}{2}\binom{2m}{k} + \binom{m}{\frac{k}{2}}.$

   (b) *If $\frac{k}{2}$ is even, that implies* $\displaystyle\sum_{\substack{j=0 \\ j \textit{ is odd}}}^{k} \binom{m}{j}\binom{m}{k-j} = \frac{1}{2}\binom{2m}{k} - \binom{m}{\frac{k}{2}}.$

3 Few classes of WAPB Boolean functions

In this section, we provide several constructions for n-variable of WAPB Boolean functions. In the paper [MS21], Mesnager and Su have proposed a WPB Boolean function over $n = 2^m$ variables using an iterative method (see 2.10 to build its support. We have generalized idea to construction WAPB functions on any variable n in Theorem 3.6 and Theorem 3.7. The following results are needed to prove the Theorems.

Lemma 3.1. *Let n be an odd integer. For $k \in [0, n]$,*

1. *if $k \not\preceq n$, then $k \not\preceq n-1$ and $k-1 \not\preceq n-1$.*
2. *if $k \preceq n$ and*
   (a) *k is odd, then $k \not\preceq n-1$ and $k-1 \preceq n-1$;*
   (b) *k is even, then $k \preceq n-1$ and $k-1 \not\preceq n-1$.*

Proof. Let the binary expansion of n and k be $n = \sum_{i=0}^{l} n_i 2^i$ and $k = \sum_{i=0}^{l} k_i 2^i$ where $n_i, k_i \in \{0, 1\}$ for $i \in [0, l]$. Further consider the binary expansion of $n-1$ and $k-1$ be $n-1 = \sum_{i=0}^{l} n'_i 2^i$ and $k = \sum_{i=0}^{l} k'_i 2^i$ where $n'_i, k'_i \in \{0, 1\}$ for $i \in [0, l]$. As n is odd, $n_0 = 1$, $n'_0 = 0$ and $n_i = n'_i$ for $i \in [1, l]$

1. As $k \not\preceq n$, $k_s > n_s$ for some $s \in [1, l]$. As $n'_s = n_s$, $k_s > n'_s$. So, $k \not\preceq n-1$.

   If k is odd then in the binary expansion of $k-1$, $k'_0 = 0$, $k_0 = 1$, and $k'_i = k_i$ for $i \in [1, l]$. Here, it still $k'_s > n'_s$ and that implies $k-1 \not\preceq n-1$. If k is even, then $k-1$ is odd. In this case, $k'_0 = 1$ and $n'_0 = 0$. So, $k-1 \not\preceq n-1$.

2. As $k \preceq n$, $k_i \le n_i$, $\forall i \in [0, l]$. If k is odd, $k-1$ is even. Then $k'_0 = 0$ and $n'_0 = 0$ and other bits satisfies $k'_i \le n'_i$, $\forall i \in [1, l]$. Hence, $k-1 \preceq n-1$. As k is odd, $n'_0 < k_0$. So, $k \not\preceq n-1$.

   Similarly, if k is even, $k_0 = n'_0 = 0$ and $k_i \le n'_i = n_i \forall i \in [1, l]$. That implies, $k \preceq n-1$. Further, since $n'_0 = 0$ and $k'_0 = 1$, $k-1 \not\preceq n-1$.

□

Lemma 3.2. *Let $n > 1$ be an odd integer and $g, h \in \mathcal{B}_{n-1}$ be two WAPB Boolean functions. Then $f \in \mathcal{B}_n$ defined as*

$$f(x_1, x_2, \ldots, x_n) = (1 + x_n) g(x_1, x_2, \ldots, x_{n-1}) + x_n h(x_1, x_2, \ldots, x_{n-1})$$
$$i.e., \ \mathtt{sup}(f) = \{(x, 0) \in \mathbb{F}_2^n : x \in \mathtt{sup}(g)\} \cup \{(y, 1) \in \mathbb{F}_2^n : y \in \mathtt{sup}(h)\}$$

is a WAPB Boolean function.

Proof. Since $g, h \in \mathcal{B}_{n-1}$ are WAPB Boolean functions, $\mathtt{wt}_k(g) = \dfrac{\binom{n-1}{k} + b_k^{n-1}}{2}$ and $\mathtt{wt}_k(h) = \dfrac{\binom{n-1}{k} + c_k^{n-1}}{2}$ for $k \in [0, n-1]$ where

$$b_k^{n-1} = \begin{cases} 0, & \text{if } k \not\preceq n-1, \\ \pm 1, & \text{if } k \preceq n-1 \end{cases} \quad \text{and} \quad c_k^{n-1} = \begin{cases} 0, & \text{if } k \not\preceq n-1, \\ \pm 1, & \text{if } k \preceq n-1. \end{cases}$$

As f is defined, we have

$$\mathtt{wt}_0(f) = \mathtt{wt}_0(g) = \frac{\binom{n-1}{0} + b_0^{n-1}}{2} = \frac{\binom{n}{0} + b_0^{n-1}}{2}$$

and

$$\mathtt{wt}_n(f) = \mathtt{wt}_{n-1}(h) = \frac{\binom{n-1}{n-1} + c_{n-1}^{n-1}}{2} = \frac{\binom{n}{n} + c_{n-1}^{n-1}}{2}.$$

Further, for $k \in [1, n-1]$, we have

$$\mathtt{sup}_k(f) = \{(x, 0) : x \in \mathtt{sup}_k(g)\} \cup \{(y, 1) : y \in \mathtt{sup}_{k-1}(h)\}.$$

That implies,

$$\begin{aligned}\mathtt{wt}_k(f) &= \mathtt{wt}_k(g) + \mathtt{wt}_{k-1}(h)\\ &= \frac{1}{2}\left[\binom{n-1}{k-1} + b_k^{n-1}\right] + \frac{1}{2}\left[\binom{n-1}{k-1} + c_{k-1}^{n-1}\right]\\ &= \frac{1}{2}\left[\binom{n}{k} + a_k^n\right]; \qquad \textit{where } a_k^n = b_k^{n-1} + c_{k-1}^{n-1}.\end{aligned}$$

- If $k \not\preceq n$, then using Lemma 3.1, $k \not\preceq n-1$ and $k-1 \not\preceq n-1$. Then $b_k^{n-1} = c_{k-1}^{n-1} = 0$. Hence, $a_k^n = 0$ i.e., $\mathtt{wt}_k(f) = \frac{1}{2}\binom{n}{k}$.
- If $k \preceq n$, then from Lemma 3.1,
  - if k is odd, then $k \not\preceq n-1$ and $k-1 \preceq n-1$. Then $b_k^{n-1} = 0$ and $c_{k-1}^{n-1} \neq 0$. Hence $a_k^n = c_{k-1}^{n-1}$ i.e., $\mathtt{wt}_k(f) = \frac{1}{2}\left(\binom{n}{k} + c_{k-1}^{n-1}\right)$.
  - if k is even, then $k \preceq n-1$ and $k-1 \not\preceq n-1$. Then $b_k^{n-1} \neq 0$ and $c_{k-1}^{n-1} = 0$. Then, $a_k^n = b_k^{n-1}$ i.e., $\mathtt{wt}_k(f) = \frac{1}{2}\left(\binom{n}{k} + b_k^{n-1}\right)$.

Hence, $f \in \mathcal{B}_n$ is a WAPB Boolean function with $\mathtt{wt}_k(f) = \dfrac{\binom{n}{k} + a_k^{n-1}}{2}$ where

$$a_k^n = \begin{cases} 0, & \textit{if } k \not\preceq n,\\ b_k^{n-1}, & \textit{if } k \preceq n \textit{ and even},\\ c_{k-1}^{n-1}, & \textit{if } k \preceq n \textit{ and odd},\\ c_{n-1}^{n-1}, & \textit{if } k = n.\end{cases}$$

□

The following is a construction of a 2^m+1-variable WAPB Boolean function from two 2^m-variable WPB Boolean functions.

Corollary 3.3. *Let $n = 2^m \geq 2$ and $g, h \in \mathcal{B}_n$ be two WPB Boolean functions. Then $f \in \mathcal{B}_{n+1}$ such that*

$$f(x_1, x_2, \dots, x_{n+1}) = (1 + x_{n+1})g(x_1, x_2, \dots, x_n) + x_{n+1}h(x_1, x_2, \dots, x_n)$$

is a WAPB Boolean function.

If $g = h$ then Lemma 3.2 is a case of the construction proposed in Proposition 2.12 for $n = 2^m+1$. Further, if we take $h = 1 + g$ in the Lemma 3.2 then the following corollary is useful for our main construction.

Corollary 3.4. *Let $n > 1$ be an odd integer and $f_{n-1} \in \mathcal{B}_{n-1}$ is a WAPB Boolean function. Then $f_n \in \mathcal{B}_n$ defined as*

$$\begin{aligned} f_n(x_1, x_2, \dots, x_n) &= (1 + x_n)f_{n-1}(x_1, x_2, \dots, x_{n-1}) + x_n(1 + f_{n-1}(x_1, x_2, \dots, x_{n-1}))\\ &= x_n + f_{n-1}(x_1, x_2, \dots, x_{n-1})\end{aligned}$$

$$\textit{i.e., } \mathtt{sup}(f_n) = \{(x, 0) \in \mathbb{F}_2^n : x \in \mathtt{sup}(f_{n-1})\} \cup \{(x, 1) \in \mathbb{F}_2^n : x \notin \mathtt{sup}(f_{n-1})\}$$

is a WAPB Boolean function.

If we denote $\mathtt{wt}_k(f_n) = \frac{\binom{n}{k} + a_k^n}{2}$ and $\mathtt{wt}_k(f_{n-1}) = \frac{\binom{n-1}{k} + a_k^{n-1}}{2}$, then

$$a_k^n = \begin{cases} 0, & \textit{if } k \not\preceq n,\\ a_k^{n-1}, & \textit{if } k \preceq n \textit{ and even},\\ -a_{k-1}^{n-1}, & \textit{if } k \preceq n \textit{ and odd},\\ -a_{n-1}^{n-1}, & \textit{if } k = n.\end{cases}$$

Lemma 3.5. *Let $n = n_0 2^m$ where n_0 be an odd positive integer and $m \geq 0$ be an integer. Let $f_{n_0} \in \mathcal{B}_{n_0}$ be a WAPB Boolean function. Then $f_n \in \mathcal{B}_n$, recursively defined as*

$$\mathtt{sup}(f_n) = \begin{cases} \mathtt{sup}(f_{n_0}) & \textit{if } n = n_0 \textit{ is odd },\\ \{(x,y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \textit{ is odd}\} \triangle \{(z,z) \in \mathbb{F}_2^n : z \in \mathtt{sup}(f_{\frac{n}{2}})\}, & \textit{if } n \textit{ is even,} \end{cases}$$

is a WAPB Boolean function.

Proof. The proof follows the idea to the proof of [MS21, Theorem 3]. As f_{n_0} is a WAPB Bollean function, $\mathtt{wt}_k(f_{n_0}) = \dfrac{\binom{n_0}{k} + a_k^{n_0}}{2}$ such that $a_k^{n_0} \in \{0, \pm 1\}$ for $k \in [0, n_0]$. Let $k \in [0, n]$ be factored as $k = k_0 2^b$ where k_0 is odd and $b \geq 0$ is an integer. Hence, for $k \in [0, n]$, we will prove that $\mathtt{wt}_k(f_n) = \dfrac{\binom{n}{k} + a_k^n}{2}$ where $a_k^n = \begin{cases} 0 & \textit{if } k \not\preceq n,\\ \pm 1 & \textit{if } k \preceq n. \end{cases}$ We will prove it in two different cases i.e, (1) $m > b$ and (2) $m \leq b$.

If $m > b$ (in this case kc), then

$$\begin{aligned}
\mathtt{sup}_k(f_n) &= \{(x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = k\} \triangle \{(z,z) : z \in \mathtt{sup}_{\frac{k}{2}}(f_{\frac{n}{2}})\}\\
&= \{(x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = k\}\\
&\quad \triangle \{(x,y,x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2^2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = \frac{k}{2}\}\\
&\quad \triangle \{(z,z,z,z) : z \in \mathtt{sup}_{\frac{k}{2^2}}(f_{\frac{n}{2^2}})\}\\
&= \{(x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = k\}\\
&\quad \triangle \{(x,y,x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2^2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = \frac{k}{2}\}\\
&\quad \vdots\\
&\quad \triangle \{(x,y,x,y,\ldots,x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2^b}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = \frac{k}{2^{b-1}}\}\\
&\quad \triangle \{(z,z,\ldots,z,z) : z \in \mathtt{sup}_{\frac{k}{2^b}}(f_{\frac{n}{2^b}})\}\\
&= \{(x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = k\} && (S_1)\\
&\quad \triangle \{(x,y,x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2^2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = \frac{k}{2}\} && (S_2)\\
&\quad \vdots\\
&\quad \triangle \{(x,y,x,y,\ldots,x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2^b}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = \frac{k}{2^{b-1}}\} && (S_b)\\
&\quad \triangle \{(x,y,x,y\ldots,x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2^{b+1}}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = \frac{k}{2^b}\} && (S_{b+1})
\end{aligned}$$

Here, we stop at S_{b+1} as $\frac{k}{2^{b+1}}$ is not an integer. As $\mathtt{wt}(x)$ is odd in the set S_1 and $\mathtt{wt}(x,y) = \frac{k}{2}$ is even in the set S_2 in the above identity, the sets S_1 and S_2 are disjoint. Similarly, we can check that the set S_3 is pairwise disjoint with the sets S_1 and S_2. Continuing the argument, we have that the set $S_j, j \in [2, b]$ is pairwise disjoint with $S_1, S_2, \ldots, S_{j-1}$ i.e., the sets $S_j, j \in [1, b]$ are mutually disjoint. Further, since the $\mathtt{wt}(x,y) = \frac{k}{2^b} = k_0$ is odd in the set S_{b+1}, the set $S_{b+1} \subset S_b$. Therefore,

$$\mathtt{wt}_k(f_n) = |S_1| + |S_2| + \cdots + |S_b| - |S_{b+1}|.$$

Here, we can check that

$$\begin{aligned}
|S_j| &= |\{(x,y,x,y,\ldots,x,y) : x,y \in \mathbb{F}_2^{\frac{n}{2^j}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = \frac{k}{2^{j-1}}\}| \\
&= \sum_{\substack{i=0 \\ i \text{ is odd}}}^{\frac{k}{2^{j-1}}} \binom{\frac{n}{2^j}}{i}\binom{\frac{n}{2^j}}{\frac{k}{2^{j-1}}-i} \\
&= \begin{cases}
\frac{1}{2}\binom{\frac{n}{2^{j-1}}}{\frac{k}{2^{j-1}}} - \frac{1}{2}\binom{\frac{n}{2^j}}{\frac{k}{2^j}} & \textit{if } j \in [1,b-1] \qquad \textit{(using Lemma 2.13[Item 2b])}, \\
\frac{1}{2}\binom{\frac{n}{2^{b-1}}}{\frac{k}{2^{b-1}}} + \frac{1}{2}\binom{\frac{n}{2^b}}{\frac{k}{2^b}} & \textit{if } j = b, \qquad \textit{(using Lemma 2.13[Item 2a])}, \\
\frac{1}{2}\binom{\frac{n}{2^b}}{\frac{k}{2^b}} & \textit{if } j = b+1 \qquad \textit{(using Lemma 2.13[Item 1])}.
\end{cases}
\end{aligned}$$

Therefore,

$$\mathtt{wt}_k(f_n) = \frac{1}{2}\left[\sum_{j=1}^{b-1}\left(\binom{\frac{n}{2^{j-1}}}{\frac{k}{2^{j-1}}} - \binom{\frac{n}{2^j}}{\frac{k}{2^j}}\right) + \binom{\frac{n}{2^{b-1}}}{\frac{k}{2^{b-1}}} + \binom{\frac{n}{2^b}}{\frac{k}{2^b}} - \binom{\frac{n}{2^b}}{\frac{k}{2^b}}\right] = \frac{1}{2}\binom{n}{k}.$$

If $m \leq b$, then using similar process as the above case we have

$$\begin{aligned}
\mathtt{sup}_k(f_n) &= \{(x,y) : x,y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = k\} \\
&\quad \triangle\{(x,y,x,y) : x,y \in \mathbb{F}_2^{\frac{n}{2^2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = \frac{k}{2}\} \\
&\quad \vdots \\
&\quad \triangle\{(x,y,x,y,\ldots,x,y) : x,y \in \mathbb{F}_2^{\frac{n}{2^m}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = \frac{k}{2^{m-1}}\} \\
&\quad \triangle\{(z,z,\ldots,z,z) : z \in \mathtt{sup}_{\frac{k}{2^m}}(f_{\frac{n}{2^m}})\} \\
&= \{(x,y) : x,y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = k\} && (T_1) \\
&\quad \triangle\{(x,y,x,y) : x,y \in \mathbb{F}_2^{\frac{n}{2^2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = \frac{k}{2}\} && (T_2) \\
&\quad \vdots \\
&\quad \triangle\{(x,y,x,y,\ldots,x,y) : x,y \in \mathbb{F}_2^{\frac{n}{2^m}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = \frac{k}{2^{m-1}}\} && (T_m) \\
&\quad \triangle\{(z,z,\ldots,z,z) : z \in \mathtt{sup}_{\frac{k}{2^m}}(f_{n_0})\} && (T_{m+1})
\end{aligned}$$

It can be checked (as the earlier way) that the sets $T_1, T_2, \ldots, T_m$ are pairwise disjoint. If $\frac{k}{2^m}$ is even (i.e., $b > m$), then $\mathtt{wt}(z)$ is even in T_{m+1}. So, T_{m+1} is too disjoint with $T_i, i \in [1,m]$. Hence,

$$\mathtt{wt}_k(f_n) = |T_1| + |T_2| + \cdots + |T_m| + |T_{m+1}|.$$

Here,

$$|T_j| = \begin{cases}
\frac{1}{2}\left(\binom{\frac{n}{2^{j-1}}}{\frac{k}{2^{j-1}}} - \binom{\frac{n}{2^j}}{\frac{k}{2^j}}\right) & \textit{if } j \in [1,m] \qquad \textit{(using Lemma 2.13[Item 2b])}, \\
\frac{1}{2}\left(\binom{\frac{n}{2^m}}{\frac{k}{2^m}} + a^{n_0}_{\frac{k}{2^m}}\right) & \textit{if } j = m+1 \qquad \textit{(as } f_{n_0} \textit{ is WAPB with } \mathtt{wt}_l(f_{n_0}) = \frac{1}{2}\left(\binom{n_0}{k} + a_l^{n_0}\right)\textit{)}.
\end{cases}$$

Hence

$$\mathtt{wt}_k(f_n) = \frac{1}{2}\sum_{j=1}^{m}\left(\binom{\frac{n}{2^{j-1}}}{\frac{k}{2^{j-1}}} - \frac{1}{2}\binom{\frac{n}{2^j}}{\frac{k}{2^j}}\right) + \frac{1}{2}\left(\binom{\frac{n}{2^m}}{\frac{k}{2^m}} + a^{n_0}_{\frac{k}{2^m}}\right) = \frac{1}{2}\left(\binom{n}{k} + a^{n_0}_{\frac{k}{2^m}}\right).$$

Further, if $\frac{k}{2^m}$ is odd (i.e., $b = m$), then $\mathtt{wt}(z)$ is odd in T_{m+1}. As $\frac{k}{2^{m-1}}$ is even, $\mathtt{wt}(x)$ and $\mathtt{wt}(y)$ are also odd in the set T_m. Hence, $T_{m+1} \subset T_m$. That implies,

$$\mathtt{wt}_k(f_n) = |T_1| + |T_2| + \cdots + |T_m| - |T_{m+1}|.$$

Here,

$$|T_j| \quad = \quad \begin{cases} \frac{1}{2}\binom{\frac{n}{2^{j-1}}}{\frac{k}{2^{j-1}}} - \frac{1}{2}\binom{\frac{n}{2^j}}{\frac{k}{2^j}} & \textit{if } j \in [1, m-1] \qquad \textit{(using Lemma 2.13[Item 2b])}, \\[2ex] \frac{1}{2}\binom{\frac{n}{2^{m-1}}}{\frac{k}{2^{m-1}}} + \frac{1}{2}\binom{\frac{n}{2^m}}{\frac{k}{2^m}} & \textit{if } j = m \qquad \textit{(using Lemma 2.13[Item 2a])}, \\[2ex] \frac{1}{2}\left(\binom{\frac{n}{2^m}}{\frac{k}{2^m}} + a^{n_0}_{\frac{k}{2^m}}\right) & \textit{if } j = m+1 \qquad (\textit{as } f_{n_0} \textit{ is WAPB with } \mathtt{wt}_l(f_{n_0}) = \frac{1}{2}\left(\binom{n_0}{k} + a^{n_0}_l\right)). \end{cases}$$

Hence

$$\mathtt{wt}_k(f_n) = \frac{1}{2}\sum_{j=1}^{m-1}\left(\binom{\frac{n}{2^{j-1}}}{\frac{k}{2^{j-1}}} - \frac{1}{2}\binom{\frac{n}{2^j}}{\frac{k}{2^j}}\right) + \frac{1}{2}\left(\binom{\frac{n}{2^{m-1}}}{\frac{k}{2^{m-1}}} + \binom{\frac{n}{2^m}}{\frac{k}{2^m}}\right) - \frac{1}{2}\left(\binom{\frac{n}{2^m}}{\frac{k}{2^m}} + a^{n_0}_{\frac{k}{2^m}}\right) = \frac{1}{2}\left(\binom{n}{k} - a^{n_0}_{\frac{k}{2^m}}\right).$$

Therefore, for $n = n_0 2^m$ and $k = k_0 2^b$, we got that $\mathtt{wt}_k(f_n) = \frac{1}{2}\left(\binom{n}{k} + a^n_k\right)$, where

$$a^n_k = \begin{cases} 0 & \textit{if } m > b, \\ a^{n_0}_{\frac{k}{2^m}} & \textit{if } m < b, \\ -a^{n_0}_{\frac{k}{2^m}} & \textit{if } m = b. \end{cases}$$

Hence, it is proved that f_n is a WAPB Boolean function if f_{n_0} is a WAPB Boolean function. □

Now we can present general constructions for WAPB Boolean functions on any number of variables using the Corollary 3.4 and Lemma 3.5.

Theorem 3.6. *For $n \geq 2$, the support of an n variable Boolean function is defined as*

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

is a WAPB Boolean function.

When $n = 2^m$, is a power of 2, we get the WPB function presented in [MS21]. The base Boolean function used in the above recursive construction (i.e., f_2) is a linear function. As a result the nonlinearity of destined Boolean function remains weak. The construction in the Theorem 3.6 can be generalized for having good cryptographic properties from a base WAPB Boolean function on a higher variable.

Theorem 3.7. *For $p \geq 2$, let f_p be a WAPB Boolean function. Let n be a positive integer such that, for a $m \geq 0$,*

-
$$p = \lfloor \frac{n}{2^m} \rfloor \textit{ i.e, } n = a_0 2^0 + a_1 2^1 + \cdots + a_{m-1} 2^{m-1} + p 2^m \tag{2}$$

or,

- $$p+1=\lfloor\frac{n}{2^m}\rfloor \text{ i.e, } n=a_0 2^0+a_1 2^1+\cdots+a_{m-1}2^{m-1}+(p+1)2^m \text{ if } p \text{ is even.} \tag{3}$$

Then $f_n \in \mathcal{B}_n$ whose support is defined as

$$\mathtt{sup}(f_n)=\begin{cases}\mathtt{sup}(f_p) & \text{if } n=p,\\ \{(x,0)\in\mathbb{F}_2^n : x\in\mathtt{sup}(f_{n-1})\}\cup\{(x,1)\in\mathbb{F}_2^n : x\notin\mathtt{sup}(f_{n-1})\} & \text{if } n>p \text{ and odd},\\ \{(x,y)\in\mathbb{F}_2^n : x,y\in\mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \text{ is odd}\}\triangle\{(z,z)\in\mathbb{F}_2^n : z\in\mathtt{sup}(f_{\frac{n}{2}})\}, & \text{if } n>p \text{ and even},\end{cases} \tag{4}$$

is a WAPB Boolean function.

For illustration, if we have a WAPB Boolean function on 5 variables then we can construct a WAPB Boolean function on $10, 11, 20, 21, 22, 23, 40, 41, \ldots$ variables. Similarly, if we have a WAPB Boolean on 6 variables then we can construct a WAPB Boolean function on $7, 12, 13, 14, 15, 24, 25, 26, 27, \ldots$ variables.

Note 3.8. *The construction in the Theorem 3.7 can further be generalized. When n is odd, instead of using two WAPB Boolean functions f_{n-1} and $1+f_{n-1}$, one can use any two WAPB Boolean functions $g, h \in \mathcal{B}_{n-1}$ (following the Lemma 3.2) to have f_n in the recursive construction presented in the Equation 4.*

3.1 Algebraic Normal Form

Since there are two different kind of lifting during the recursive construction (i.e., when n is odd and when n is even), the ANF of the Boolean function $f_n \in \mathcal{B}_n$ depends on the binary bits of the integer n. Therefore the ANF of f_n can be computed as the following theorem.

Theorem 3.9. *For $p \geq 2$, let f_p be a WAPB Boolean function. Let n be a positive integer such that, for a $m \geq 0$,*

- $p=\lfloor\frac{n}{2^m}\rfloor$ *i.e,* $n=a_0 2^0+a_1 2^1+\cdots+a_{m-1}2^{m-1}+p2^m$,

  or,

- $p+1=\lfloor\frac{n}{2^m}\rfloor$ *i.e,* $n=a_0 2^0+a_1 2^1+\cdots+a_{m-1}2^{m-1}+(p+1)2^m$ *if p is even.*

Then the ANF of f_n, defined in the Theorem 3.7 is

$$f_n(x_1,x_2,\ldots,x_n)=\begin{cases}f_p & \text{if } n=p,\\ x_n+f_{n-1}(x_1,x_2,\ldots,x_{n-1}) & \text{if } n>p \text{ and odd},\\ \sum_{i=1}^{\frac{n}{2}}x_i+f_{\frac{n}{2}}(x_1,x_2,\ldots,x_{\frac{n}{2}})\prod_{i=1}^{\frac{n}{2}}(x_i+x_{\frac{n}{2}+i}+1) & \text{if } n>p \text{ and even},\end{cases} \tag{5}$$

is a WAPB Boolean function.

Proof. If $n=p$, then by our assumption $f_n=f_p$. Now consider that $n>p$. If n is odd then the ANF of f_n is done from the Corollary 3.4. Now if n is even, we prove it following the technique of the proof from [MS21, Theorem 4]. Here

$$\mathtt{sup}(f_n)=\{(x,y)\in\mathbb{F}_2^n : x,y\in\mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \text{ is odd}\}\triangle\{(z,z)\in\mathbb{F}_2^n : z\in\mathtt{sup}(f_{\frac{n}{2}})\}$$

Let denote $g_n, h_n \in \mathcal{B}_n$ such that

$$\mathtt{sup}(g_n)=\{(x,y)\in\mathbb{F}_2^n : x,y\in\mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \text{ is odd}\};\ \text{and } \mathtt{sup}(h_n)=\{(z,z)\in\mathbb{F}_2^n : z\in\mathtt{sup}(f_{\frac{n}{2}})\}.$$

Then the ANFs of g_n and h_n are

$$g_n(x_1,x_2,\ldots,x_n)=\sum_{i=1}^{\frac{n}{2}}x_i \text{ and } h(x_1,x_2,\ldots,x_n)=f_{\frac{n}{2}}(x_1,x_2,\ldots,x_{\frac{n}{2}})\prod_{i=1}^{\frac{n}{2}}(x_i+x_{\frac{n}{2}+i}+1).$$

As the XOR operation imitates the symmetric difference of the supports of two Boolean functions, we have

$$f_n(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{\frac{n}{2}} x_i + f_{\frac{n}{2}}(x_1, x_2, \ldots, x_{\frac{n}{2}}) \prod_{i=1}^{\frac{n}{2}} (x_i + x_{\frac{n}{2}+i} + 1).$$

□

For example, we will compute ANF of $f_{11} \in \mathcal{B}_{11}$ for a given WAPB $f_5 \in \mathcal{B}_5$. Then we will have $f_{10}(x_1, x_2, \ldots, x_{10}) = \sum_{i=1}^{5} x_i + f_5(x_1, x_2, \ldots, x_5) \prod_{i=1}^{5}(x_i + x_{5+i} + 1)$. Then we will have $f_{11}(x_1, x_2, \ldots, x_{11}) = \sum_{i=1}^{5} x_i + x_{11} + f_5(x_1, x_2, \ldots, x_5) \prod_{i=1}^{5}(x_i + x_{5+i} + 1)$. Therefore, the ANF of the WAPB functions are complex and can be computed recursively very fast.

The algebraic degree of f_n can be computed as follows.

Theorem 3.10. *Let $f_p \in \mathcal{B}_p$ be a Boolean function with $\deg(f_p) \geq 1$ and $f_n \in \mathcal{B}_n$ be the Boolean function constructed as in the Theorem 3.7. Then the algebraic degree of f_n is $\deg(f_n) = \lfloor \frac{n}{2} \rfloor + \lfloor \frac{n}{2^2} \rfloor + \cdots + \lfloor \frac{n}{2^m} \rfloor + \deg(f_p)$. That is,*

1. *$\deg(f_n) = n - (p + a_{m-1} + a_{m-2} + \cdots + a_0) + \deg(f_p)$ if $p = \lfloor \frac{n}{2^m} \rfloor$ as in the Equation 2;*
2. *$\deg(f_n) = n - (p + 1 + a_{m-1} + a_{m-2} + \cdots + a_0) + \deg(f_p)$ if $p + 1 = \lfloor \frac{n}{2^m} \rfloor$ as in the Equation 3.*

Proof. If $a_0 = 1$ (i.e., n is odd) then $f_n(x_1, x_2, \ldots, x_n) = x_n + f_{n-1}(x_1, x_2, \ldots, x_{n-1})$. Hence, $\deg(f_n) = \deg(f_{n-a_0})$ irrespective of $a_0 = 0$ or 1.

Further, if n is even (i.e., $a_0 = 0$) then $f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{\frac{n}{2}} x_i + f_{\frac{n}{2}}(x_1, x_2, \ldots, x_{\frac{n}{2}}) \prod_{i=1}^{\frac{n}{2}}(x_i + x_{\frac{n}{2}+i} + 1)$ as per the construction. That implies $\deg(f_n) = \frac{n}{2} + \deg(f_{\frac{n}{2}})$. Therefore, doing this process recursively, we will have

$$\begin{aligned}
\deg(f_n) &= \deg(f_{n-a_0}) = \frac{n - a_0}{2} + \deg(f_{\frac{n-a_0}{2}}) = \lfloor \frac{n}{2} \rfloor + \deg(f_{\lfloor \frac{n}{2} \rfloor}) \\
&= \lfloor \frac{n}{2} \rfloor + \deg(f_{\lfloor \frac{n}{2} \rfloor - a_1}) = \lfloor \frac{n}{2} \rfloor + \frac{\lfloor \frac{n}{2} \rfloor - a_1}{2} + \deg(f_{\frac{\lfloor \frac{n}{2} \rfloor - a_1}{2}}) = \lfloor \frac{n}{2} \rfloor + \lfloor \frac{n}{2^2} \rfloor + \deg(f_{\lfloor \frac{n}{2^2} \rfloor}) \\
&\vdots \\
&= \lfloor \frac{n}{2} \rfloor + \lfloor \frac{n}{2^2} \rfloor + \cdots + \lfloor \frac{n}{2^m} \rfloor + \deg(f_{\lfloor \frac{n}{2^m} \rfloor}) \\
&= \lfloor \frac{n}{2} \rfloor + \lfloor \frac{n}{2^2} \rfloor + \cdots + \lfloor \frac{n}{2^m} \rfloor + \deg(f_p) \qquad \text{(if } p \text{ is even, still } \deg(f_{p+1}) = \deg(f_p)\text{)}.
\end{aligned}$$

If $p = \lfloor \frac{n}{2^m} \rfloor$ (as the Equation 2), $\lfloor \frac{n}{2^k} \rfloor = p2^{m-k} + a_{m-1}2^{m-1-k} + \cdots + a_k$ for $0 \leq k \leq m$. Then, substituting $\lfloor \frac{n}{2^k} \rfloor$ for $1 \leq k \leq m$ in the above equation we will have $\deg(f_n) = n - (p + a_{m-1} + a_{m-2} + \cdots + a_0) + \deg(f_p)$. Similarly, for the case as in the Equation 3, we will have $\deg(f_n) = n - (p + 1 + a_{m-1} + a_{m-2} + \cdots + a_0) + \deg(f_p)$. □

The following corollary presents the degree of f_n (constructed as in the Theorem 3.6) for some speacial n.

Corollary 3.11. *For $n \geq 2$, consider the WAPB Boolean function $f_n \in \mathcal{B}_n$ as in the Theorem 3.6. The degree of f_n is*

1. *$n - 1$ if $n = 2^k$ for some $k \geq 1$ (i.e., n is a power of 2) [MS21, Corollary 3];*
2. *$n - k$ if $n = 2^k - 1$ for some $k \geq 2$.*

Proof. 1. Here $p = 2$ as per the Theorem 3.6 and $n = 2^k$. That is, $m = k - 1$ and $a_{m-1} = \cdots = a_0 = 0$. So $\deg(f_n) = n - p + \deg(f_2) = n - 2 + 1 = n - 1$.

2. Here $p = 2$ as per the Theorem 3.6 and $n = 2^k - 1 = (2+1)2^{k-2} + 2^{k-3} + \cdots + 2^1 + 1$. That implies, $m = k - 2$ and $a_{m-1} = \cdots = a_0 = 1$. So $\deg(f_n) = n - (p + 1 + (a_{m-1} + \cdots + a_0)) + \deg(f_2) = n - (2 + 1 + m) + 1 = n - 2 - (k - 2) = n - k$.

□

3.2 Nonlinearity

Nonlinearity is a very important cryptographic properties of Boolean functions. In this subsection we will study the nonlinearity of our proposed WAPB Boolean functions. Since there are two different kind of lifting in the recursive construction, we will present the nonlinearity bound for the both cases.

Lemma 3.12. *Let $f_n \in \mathcal{B}_n$ such $f_n(x_1, x_2, \cdots, x_n) = x_n + f_{n-1}(x_1, x_2, \cdots, x_{n-1})$ for a $f_{n-1} \in CB_n$. Then $\mathtt{nl}(f_n) = 2\mathtt{nl}(f_{n-1})$.*

Proof. Let $a_{n-1} \in \mathcal{B}_{n-1}$ be an affine function such that $\mathtt{d}(f_{n-1}, a_{n-1}) = \mathtt{nl}(f_{n-1})$. Then $\mathtt{d}(f_n, x_n + a_{n-1}) = 2\mathtt{nl}(f_{n-1})$. That implies $\mathtt{nl}(f_n) \leq 2\mathtt{nl}(f_{n-1})$.

In other direction, let $a_n \in \mathcal{B}_n$ be an affine function such that $\mathtt{d}(f_n, l_n) = \mathtt{nl}(f_n)$. Consider that $a_n = (1 + x_n)b_{n-1} + x_n c_{n-1}$ where $b_{n-1}, c_{n-1} \in CB_{n-1}$ are two affine functions. Then $\mathtt{d}(f_{n-1}, b_{n-1}) \leq \frac{\mathtt{nl}(f_n)}{2}$ or, $\mathtt{d}(1 + f_{n-1}, c_{n-1}) = \mathtt{d}(f_{n-1}, 1 + c_{n-1}) \leq \frac{\mathtt{nl}(f_n)}{2}$. That implies, $\mathtt{nl}(f_{n-1}) \leq \frac{\mathtt{nl}(f_n)}{2}$, i.e., $\mathtt{nl}(f_n) \geq 2\mathtt{nl}(f_{n-1})$. Hence, $\mathtt{nl}(f_n) = 2\mathtt{nl}(f_{n-1})$. □

Lemma 3.13. *Let $n > 0$ be an even integer and $f_n \in \mathcal{B}_n$ such that*

$$\mathtt{sup}(f_n) = \{(x, y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \textit{ is odd}\} \triangle \{(z, z) \in \mathbb{F}_2^n : z \in \mathtt{sup}(f_{\frac{n}{2}})\} \textit{ where } f_{\frac{n}{2}} \in \mathcal{B}_{\frac{n}{2}}.$$

Then $\mathtt{nl}(f_n) \leq \mathtt{wt}(f_{\frac{n}{2}})$.

Proof. Consider $g, h \in \mathcal{B}_n$ such that $\mathtt{sup}(g) = \{(x, y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \textit{ is odd}\}$ and $\mathtt{sup}(h) = \{(z, z) \in \mathbb{F}_2^n : z \in \mathtt{sup}(f_{\frac{n}{2}})\}$. Then $f_n = g + h$ and $g = x_1 + x_2 + \cdots + x_{\frac{n}{2}}$ is a linear function. Therefore, $\mathtt{d}(f_n, g) = \mathtt{wt}(h) = |\{(z, z) \in \mathbb{F}_2^n : z \in \mathtt{sup}(f_{\frac{n}{2}})\}| = \mathtt{wt}(f_{\frac{n}{2}})$. That implies, $\mathtt{nl}(f_n) \leq \mathtt{wt}(f_{\frac{n}{2}})$. □

If $f_{\frac{n}{2}}$ is a balance function, then $\mathtt{nl}(f_n) \leq \mathtt{wt}(f_{\frac{n}{2}}) = 2^{\frac{n}{2}-1}$. This lifting is very discouraging in terms of nonlinearity. Therefore, the proposed construction is having very poor nonlinearity. This result happens due to the addition of the linear part $\{(x, y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \textit{ is odd}\}$. The researchers may be interested whether it is possible to get WAPB function by substituting the linear part a very nonlinear part. Further, we have a discouraging result for wightwise nonlinearity.

Corollary 3.14. *If n is even and $n > p$ then $\mathtt{nl}_k(f_n) = 0$ for all odd integer $k \in [0, n]$.*

Proof. Consider the functions g, h as in the proof of the Lemma 3.13. Then $\mathtt{sup}_k(h) = \phi$ for every odd $k \in [0, n]$. Therefore, $f_n = g$ which is a linear function and hence $\mathtt{nl}_k(f_n) = 0$ for all odd $k \in [0, n]$. □

The following table presents the nonlinearity and weight nonlinearity of the functions for $n = 10, 11, 12, 13, 14$ which are generated using the Theorem 3.6.

n	$\mathtt{nl}$	$\mathtt{nl}_0$	$\mathtt{nl}_1$	$\mathtt{nl}_2$	$\mathtt{nl}_3$	$\mathtt{nl}_4$	$\mathtt{nl}_5$	$\mathtt{nl}_6$	$\mathtt{nl}_7$	$\mathtt{nl}_8$	$\mathtt{nl}_9$	$\mathtt{nl}_{10}$	$\mathtt{nl}_{11}$	$\mathtt{nl}_{12}$	$\mathtt{nl}_{13}$	$\mathtt{nl}_{14}$
10	$16 = 2^4$	0	0	3	0	5	0	5	0	3	0	0	–	–	–	–
11	32	0	0	3	3	5	5	5	5	3	3	0	0	–	–	–
12	$32 = 2^5$	0	0	3	0	7	0	10	0	8	0	3	0	0	–	–
13	64	0	0	3	3	7	7	10	10	8	8	3	3	0	0	–
14	$64 = 2^6$	0	0	4	0	10	0	18	0	18	0	10	0	4	0	0

Similarly, we have a construction of a 2^m-variable WPB Boolean function from two $2^m - 1$ WAPB Boolean functions.

Theorem 3.15. *Let $n = 2^m \geq 2$ and $g, g' \in \mathcal{B}_{n-1}$ be two WAPB with Hamming weight $\mathtt{wt}_k(g) = \mathtt{wt}_k(g') = \frac{\binom{n-1}{k}+(-1)^k}{2}$ for $k \in [0, n-1]$. Then $f \in \mathcal{B}_n$ such that*

$$f(x_1, x_2, \ldots, x_n) = (1 + x_n)g(x_1, x_2, \ldots, x_{n-1}) + x_n g'(x_1, x_2, \ldots, x_{n-1})$$

is a WPB Boolean function.

Proof. Here, $f(x_1, x_2, \ldots, x_n) = \begin{cases} g(x_1, x_2, \ldots, x_{n-1}) & \text{for } \; x_n = 0, \\ g'(x_1, x_2, \ldots, x_{n-1}) & \text{for } \; x_n = 1. \end{cases}$ For $k \in [1, n]$, $x \in E_{n,k}$ is of the form $x = x'||0$ for $x' \in E_{n-1,k}$ or $x = x'||1$ for $x' \in E_{n-1,k-1}$. Hence, for $x \in E_{n,k}$, $f(x) = g(x')$ if $x = x'||0$ with $x' \in E_{n-1,k}$ or, $f(x) = g'(x')$ if $x = x'||1$ with $x' \in E_{n-1,k-1}$. So, $\mathtt{wt}_k(f) = \mathtt{wt}_k(g) + \mathtt{wt}_{k-1}(g')$ for $k \in [1, n]$. For $k \in [1, n-1]$, $\mathtt{wt}_k(f) = \mathtt{wt}_k(g) + \mathtt{wt}_{k-1}(g') = \frac{\binom{n-1}{k}+(-1)^k}{2} + \frac{\binom{n-1}{k-1}+(-1)^{k-1}}{2} = \frac{\binom{n}{k}}{2}$. Hence, f is WPB Boolean function on $n = 2^m$ variables. □

4 Algebraic Immunity

Let $E \subseteq \mathbb{F}_2^n$ and f, g be two n-variable Boolean functions defined over E. Then, g is said to be an annihilator of f over E,if $g(x)f(x) = 0$ holds. If $E = \mathbb{F}_2^n$, then g is said to be an annihilator of f over $\mathbb{F}_2^n$ if $g(x)f(x) = 0$ forall $x \in \mathbb{F}_2^n$.

So, the algebraic immunity of a Boolean function f over $\mathbb{F}_2^n$ is defined as

$$AI(f) = min\{deg(g) : f(x).g(x) = 0 \text{ or } (f(x) + 1).g(x) = 0; g(x) \neq 0 \text{ over } \mathbb{F}_2^n\}$$

So,it can be concluded that, the annihilator $g(x)$ of $f(x)$ over $\mathbb{F}_2^n$ is also an annihilator $f(x)$, when f is restricted E. Hence, $AI_E(f) \leq AI(f)$.

Definition 4.1. *Let $E \subseteq \mathbb{F}_2^n$. The algebraic immunity of a function f over E, denoted by $AI_E(f) = min\{deg(g) : f(x).g(x) = 0$ or $(f(x) + 1).g(x) = 0; g(x) \neq 0$ over $E\}$.*

Proposition 4.2. *Let $E \subseteq \mathbb{F}_2^n$ and $f(x) = x_n f_1(x) + (1 + x_n)f_2(x)$, a Boolean function of n-variable where $f_1(x), f_2(x)$ be Boolean functions of $n-1$-variable. Then there exists $n-1$-variable Boolean function g_1 and g_2, an annihilator of f_1 and f_2 respectively, such that $g(x) = x_n g_1(x) + (1 + x_n)g_2(x)$ is an annihilator of $f(x)$.*

Theorem 4.3. *Let $n > 0$ be an even integer and $f_n \in \mathcal{B}_n$ such that*

$$\mathtt{sup}(f_n) = \{(x, y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \textit{ is odd}\} \triangle \{(z, z) \in \mathbb{F}_2^n : z \in \mathtt{sup}(f_{\frac{n}{2}})\} \textit{ where } f_{\frac{n}{2}} \in \mathcal{B}_{\frac{n}{2}}.$$

Then $AI(f) \leq 2$.

Proof. In Theorem 3.9, the ANF of the above defined f_n is given by

$$f_n(x) = \sum_{i=1}^{\frac{n}{2}} x_i + f_{\frac{n}{2}}(x_1, x_2, \ldots, x_{\frac{n}{2}}) \prod_{i=1}^{\frac{n}{2}} (x_i + x_{\frac{n}{2}+i} + 1)$$

Let $g(x) = (1 + \sum_{i=1}^{\frac{n}{2}} x_i)(1 + x_1 + x_{\frac{n}{2}+1} + 1)$. Then, $f_n(x).g(x) = 0$ for all $x \in \sup(f_n)$. Hence, $AI(f_n) \leq 2$. □

The algebraic immunity of the Boolean function in Theorem 3.9 over $\mathbb{F}_2^n$ is poor.

Construction 1 Let $n = n_0 2^m$ where n_0 be an odd positive integer and $m \geq 1$ be an integer. Let $f_{n_0} \in \mathcal{B}_{n_0}$ be a WAPB Boolean function. The $f_n \in \mathcal{B}_n$, recursively defined in Lemma 3.5 as

$$\mathtt{sup}(f_n) = \begin{cases} \mathtt{sup}(f_{n_0}) & \textit{if } n = n_0 \textit{ is odd }, \\ \{(x, y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \textit{ is odd}\} \triangle \{(z, z) \in \mathbb{F}_2^n : z \in \mathtt{sup}(f_{\frac{n}{2}})\}, & \textit{if } n \textit{ is even,} \end{cases}$$

For $k \in [0, n]$, the $\texttt{sup}(f_n)$ over $E_{n,k}$ is

$$\texttt{sup}_k(f_n) = \{(x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \texttt{wt}(x) \textit{ is odd}, \texttt{wt}(x,y) = k\} \triangle \{(z,z) : z \in \texttt{sup}_{\frac{k}{2}}(f_{\frac{n}{2}})\}$$

We define a support $\texttt{sup}_k(\bar{f_n})$ by modifying $\texttt{sup}_k(f_n)$ as follows

$$\texttt{sup}_k(\bar{f_n}) = \begin{cases} \texttt{sup}_k(f_n) & \textit{if } k \textit{ is even}, \\ \{(x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \texttt{wt}(x) \textit{ is odd}, \texttt{wt}(x,y) = k, \textit{ and for } y = (y_1, y_2, \ldots, y_{\frac{n}{2}}), y_1 = 1\} & \\ \cup\{(y,x) : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \texttt{wt}(x) \textit{ is odd}, \texttt{wt}(x,y) = k, \textit{ and for } y = (y_1, y_2, \ldots, y_{\frac{n}{2}}), y_1 = 0\} & \textit{if } k \textit{ is odd}. \end{cases} \tag{6}$$

Theorem 4.4. *The Boolean function $\bar{f_n} \in \mathcal{B}_n$ generated by Construction 1 is WAPB.*

Proof. The proof is similar to the Lemma 3.5. Let for $k \in [0, n]$, k can be written as $k = k_0 2^b$ where k_0 is odd and $b \geq 0$ be an integer. We will prove this in three different cases by taking (1) $b = 0$, (2) $m > b \geq 1$ and (3) $m \leq b$.

Case-1: If $b = 0$, then $k = k_0$, which is odd. Therefore $k \npreceq n$ as $n = n_0 2^m$ for $m \geq 1$. Then

$$\begin{aligned} \texttt{sup}_k(\bar{f_n}) &= \{(x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \texttt{wt}(x) \textit{ is odd}, y = (y_1 = 1, y_2, \ldots, y_{\frac{n}{2}}), \texttt{wt}(x,y) = k\} \\ &\quad \triangle\{(y,x) : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \texttt{wt}(x) \textit{ is odd }, y = (y_1 = 0, y_2, \ldots, y_{\frac{n}{2}}), \texttt{wt}(x,y) = k\} \\ &\quad \triangle\{(z,z) : z \in \texttt{sup}_{\frac{k}{2}}(\bar{f_{\frac{n}{2}}})\} \end{aligned}$$

Since k is odd, the set $\{(z,z) : z \in \texttt{sup}_{\frac{k}{2}}(\bar{f_{\frac{n}{2}}})\}$ is an empty set. Now, by taking

$$A = \{(x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \texttt{wt}(x) \textit{ is odd}, y = (y_1 = 1, y_2, \ldots, y_{\frac{n}{2}}), \texttt{wt}(x,y) = k\},$$

and

$$B = \{(y,x) : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \texttt{wt}(x) \textit{ is odd}, y = (y_1 = 0, y_2, \ldots, y_{\frac{n}{2}}), \texttt{wt}(x,y) = k\}.$$

We can see, $A \cap B = \phi$, as for $v_1 \in A$ and $v_2 \in B$, Hamming weight of first $\frac{n}{2}$ tuples in v_1 is odd whereas in v_2 is even. Therefore

$$\begin{aligned} \texttt{wt}_k(\bar{f_n}) &= \sum_{\substack{i=0 \\ i \text{ is odd}}}^{k} \binom{\frac{n}{2}}{i} \binom{\frac{n}{2} - 1}{(k-1) - i} + \sum_{\substack{i=0 \\ i \text{ is odd}}}^{k} \binom{\frac{n}{2}}{i} \binom{\frac{n}{2} - 1}{k - i} \\ &= \sum_{\substack{i=0 \\ i \text{ is odd}}}^{k} \binom{\frac{n}{2}}{i} \binom{\frac{n}{2}}{k - i} \\ &= \frac{1}{2} \binom{n}{k} \end{aligned}$$

Case-II: If $m > b \geq 1$, then $k = k_0 2^b$ which is even. So as we defined

$$\begin{aligned}
\mathtt{sup}_k(\bar{f_n}) &= \mathtt{sup}_k(f_n) \\
&= \{(x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = k\} \\
&\quad \triangle\{(x,y,x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2^2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = \frac{k}{2}\} \\
&\quad \vdots \\
&\quad \triangle\{(x,y,x,y,\ldots,x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2^b}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = \frac{k}{2^{b-1}}\} \\
&\quad \triangle\{(z,z,\ldots,z,z) : z \in \mathtt{sup}_{\frac{k}{2^b}}(f_{\frac{n}{2^b}})\} \\
&= \{(x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = k\} \\
&\quad \triangle\{(x,y,x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2^2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = \frac{k}{2}\} \\
&\quad \vdots \\
&\quad \triangle\{(x,y,x,y,\ldots,x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2^b}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = \frac{k}{2^{b-1}}\} \\
&\quad \triangle\{(z,z,\ldots,z,z) : z \in \mathtt{sup}_{\frac{k}{2^b}}(\bar{f}_{\frac{n}{2^b}})\} \\
&= \{(x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = k\} && (S_1) \\
&\quad \triangle\{(x,y,x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2^2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = \frac{k}{2}\} && (S_2) \\
&\quad \vdots \\
&\quad \triangle\{(x,y,x,y,\ldots,x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2^b}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x,y) = \frac{k}{2^{b-1}}\} && (S_b) \\
&\quad \triangle\{(x,y) : x, y \in \mathbb{F}_2^{\frac{n}{2^{b+1}}}, \mathtt{wt}(x) \textit{ is odd}, y = (y_1 = 1, y_2, \ldots, y_{\frac{n}{2}}), \mathtt{wt}(x,y) = \frac{k}{2^b}\} && (S_{b+1(a)}) \\
&\quad \triangle\{(y,x) : x, y \in \mathbb{F}_2^{\frac{n}{2^{b+1}}}, \mathtt{wt}(x) \textit{ is odd }, y = (y_1 = 0, y_2, \ldots, y_{\frac{n}{2}}), \mathtt{wt}(x,y) = \frac{k}{2^b}\} && (S_{b+1(b)})
\end{aligned}$$

By following the Lemma 3.5, we can see $S_i \cap S_j = \phi$ for $1 \leq i < j \leq b$. Further, since the $\mathtt{wt}(x,y) = \frac{k}{2^b} = k_0$ is odd in the sets $S_{b+1(a)}$ and $S_{b+1(b)}$, the set $S_{b+1(a)} \cup S_{b+1(b)} \subset S_b$ (where $S_{b+1(a)} \cap S_{b+1(b)} = \phi$). Therefore,

$$\mathtt{wt}_k(\bar{f_n}) = |S_1| + |S_2| + \cdots + |S_b| - |S_{b+1(a)} \cup S_{b+1(b)}|$$

The cardinality of S_j for $j \in [1, b]$ has been computed in Lemma 3.5. Now,

$$\begin{aligned}
|S_{b+1(a)} \cup S_{b+1(b)}| &= \sum_{\substack{i=0 \\ i \text{ is odd}}}^{\frac{k}{2^b}} \binom{\frac{n}{2^{b+1}}}{i} \binom{\frac{n}{2^{b+1}} - 1}{\frac{k}{2^b} - 1 - i} + \sum_{\substack{i=0 \\ i \text{ is odd}}}^{\frac{k}{2^b}} \binom{\frac{n}{2^{b+1}}}{i} \binom{\frac{n}{2^{b+1}} - 1}{\frac{k}{2^b} - i} \\
&= \sum_{\substack{i=0 \\ i \text{ is odd}}}^{\frac{k}{2^b}} \binom{\frac{n}{2^{b+1}}}{i} \binom{\frac{n}{2^{b+1}}}{\frac{k}{2^b} - i} \\
&= \frac{1}{2} \binom{\frac{n}{2^b}}{\frac{k}{2^b}}
\end{aligned}$$

Therefore,

$$\mathtt{wt}_k(f_n) = \frac{1}{2} \left[\sum_{j=1}^{b-1} \left(\binom{\frac{n}{2^{j-1}}}{\frac{k}{2^{j-1}}} - \binom{\frac{n}{2^j}}{\frac{k}{2^j}} \right) + \binom{\frac{n}{2^{b-1}}}{\frac{k}{2^{b-1}}} + \binom{\frac{n}{2^b}}{\frac{k}{2^b}} - \binom{\frac{n}{2^b}}{\frac{k}{2^b}} \right] = \frac{1}{2} \binom{n}{k}.$$

If $m < b$, then by following Lemma 3.5 we have

$$\begin{aligned}
\mathtt{sup}_k(\bar{f}_n) \quad &= \quad \{(x, y) : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x, y) = k\} && (T_1)\\
&\quad\ \triangle\{(x, y, x, y) : x, y \in \mathbb{F}_2^{\frac{n}{2^2}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x, y) = \frac{k}{2}\} && (T_2)\\
&\quad\ \vdots\\
&\quad\ \triangle\{(x, y, x, y, \ldots, x, y) : x, y \in \mathbb{F}_2^{\frac{n}{2^m}}, \mathtt{wt}(x) \textit{ is odd}, \mathtt{wt}(x, y) = \frac{k}{2^{m-1}}\}\\
&\quad\ \triangle\{(z, z, \ldots, z, z) : z \in \mathtt{sup}_{\frac{k}{2^m}}(f_{\frac{n}{2^m}})\} && (T_{m+1})
\end{aligned}$$

By following Lemma 3.5, we can see $T_i \cap T_j = \phi$ for $1 \leq i < j \leq m$. The set T_{m+1} is equal to the set T_{m+1} in Lemma 3.5 for $m < b$ and the cardinality of T_j for $j \in [1, m + 1]$ is already computed.
Hence

$$\mathtt{wt}_k(\bar{f}_n) = \frac{1}{2}\sum_{j=1}^{m}\left(\binom{\frac{n}{2^{j-1}}}{\frac{k}{2^{j-1}}} - \frac{1}{2}\binom{\frac{n}{2^j}}{\frac{k}{2^j}}\right) + \frac{1}{2}\left(\binom{\frac{n}{2^m}}{\frac{k}{2^m}} + a^{n_0}_{\frac{k}{2^m}}\right) = \frac{1}{2}\left(\binom{n}{k} + a^{n_0}_{\frac{k}{2^m}}\right).$$

Further, if $m = b$, then $\frac{k}{2^m} = k_0$ is odd. Then the set in T_{m+1} i.e.

$$\{(z, z, \ldots, z) : z \in \mathtt{sup}_{\frac{k}{2^m}}(f_{\frac{n}{2^m}})\} = \{(z, z, \ldots, z) : z \in \mathtt{sup}_{k_0}(f_{n_0})\}$$

where $\mathtt{sup}_{k_0}(f_{n_0})$ is defined. For this case, the cardinality of T_j for $j \in [1, m+1]$ is also computed in Lemma 3.5. Hence,

$$\mathtt{wt}_k(\bar{f}_n) = \frac{1}{2}\sum_{j=1}^{m-1}\left(\binom{\frac{n}{2^{j-1}}}{\frac{k}{2^{j-1}}} - \frac{1}{2}\binom{\frac{n}{2^j}}{\frac{k}{2^j}}\right) + \frac{1}{2}\left(\binom{\frac{n}{2^{m-1}}}{\frac{k}{2^{m-1}}} + \binom{\frac{n}{2^m}}{\frac{k}{2^m}}\right) - \frac{1}{2}\left(\binom{\frac{n}{2^m}}{\frac{k}{2^m}} + a^{n_0}_{\frac{k}{2^m}}\right) = \frac{1}{2}\left(\binom{n}{k} - a^{n_0}_{\frac{k}{2^m}}\right).$$

Therefore, for $n = n_0 2^m$ and $k = k_0 2^b$, we got that $\mathtt{wt}_k(\bar{f}_n) = \frac{1}{2}\left(\binom{n}{k} + a^n_k\right)$, where

$$a^n_k = \begin{cases} 0 & \textit{if } m > b,\\ a^{n_0}_{\frac{k}{2^m}} & \textit{if } m < b,\\ -a^{n_0}_{\frac{k}{2^m}} & \textit{if } m = b. \end{cases}$$

Hence, it is proved that $\bar{f}_n$ is a WAPB Boolean function if f_{n_0} is a WAPB Boolean function.

□

Theorem 4.5. *For $p \geq 2$, let f_p be a WAPB Boolean function. Let n be a positive integer such that, for a $m \geq 0$,*

- $p = \lfloor \frac{n}{2^m} \rfloor$ *i.e,* $n = a_0 2^0 + a_1 2^1 + \cdots + a_{m-1} 2^{m-1} + p 2^m$,

  or,

- $p + 1 = \lfloor \frac{n}{2^m} \rfloor$ *i.e,* $n = a_0 2^0 + a_1 2^1 + \cdots + a_{m-1} 2^{m-1} + (p + 1) 2^m$ *if p is even.*

Then the ANF of f_n, defined in the Theorem 3.7 is

$$\bar{f}_n(x_1, x_2, \ldots, x_n) = \begin{cases} f_p & \textit{if } n = p,\\ x_n + \bar{f}_{n-1}(x_1, x_2, \ldots, x_{n-1}) & \textit{if } n > p \textit{ and odd},\\ \sum_{i=1}^{\frac{n}{2}} x_i + \sum_{i=1}^{\frac{n}{2}} x_i \sum_{\frac{n}{2}+2}^{n} x_i + \bar{f}_{\frac{n}{2}}(x_1, x_2, \ldots, x_{\frac{n}{2}}) \prod_{i=1}^{\frac{n}{2}} (x_i + x_{\frac{n}{2}+i} + 1) & \textit{if } n > p \textit{ and even}, \end{cases} \tag{7}$$

is a WAPB Boolean function.

Proof. The proof is similar for $n = p$ and for n is odd when $n > p$ from the Theorem 3.9 . Now if n is even, then

$$\begin{aligned}\texttt{sup}(\bar{f}_n) = \{&(x,y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \texttt{wt}(x) \textit{ is odd}, \texttt{wt}(y) \textit{ is odd}\} \\ &\triangle\{(x,y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \texttt{wt}(x) \textit{ is odd}, \texttt{wt}(y) \textit{ is even}, y = (y_1 = 1, y_2, \ldots, y_{\frac{n}{2}})\} \\ &\triangle\{(y,x) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \texttt{wt}(x) \textit{ is odd}, \texttt{wt}(y) \textit{ is even}, y = (y_1 = 0, y_2, \ldots, y_{\frac{n}{2}})\} \\ &\triangle\{(z,z) \in \mathbb{F}_2^n : z \in \texttt{sup}(f_{\frac{n}{2}})\}\end{aligned}$$

Let g_n, h_n, $a_n, b_n \in \mathcal{B}_n$ such that

$$\begin{aligned}\texttt{sup}(g_n) &= \{(x,y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \texttt{wt}(x) \textit{ is odd}, \texttt{wt}(y) \textit{ is odd}\}; \\ \texttt{sup}(h_n) &= \{(x,y) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \texttt{wt}(x) \textit{ is odd}, \texttt{wt}(y) \textit{ is even}, y = (y_1 = 1, y_2, \ldots, y_{\frac{n}{2}})\} \\ \texttt{sup}(a_n) &= \{(y,x) \in \mathbb{F}_2^n : x, y \in \mathbb{F}_2^{\frac{n}{2}}, \texttt{wt}(x) \textit{ is odd}, \texttt{wt}(y) \textit{ is even}, y = (y_1 = 0, y_2, \ldots, y_{\frac{n}{2}})\} \text{ and} \\ \texttt{sup}(b_n) &= \{(z,z) \in \mathbb{F}_2^n : z \in \texttt{sup}(f_{\frac{n}{2}})\}\end{aligned}$$

If we denote $(x,y) = (x_1, x_2, \ldots, x_{\frac{n}{2}}, x_{\frac{n}{2}+1}, x_{\frac{n}{2}+2}, \ldots, x_n)$, then the ANFs of g_n, h_n are

$$g_n(x_1, x_2, \ldots, x_n) = (\sum_{i=1}^{\frac{n}{2}} x_i)(\sum_{i=\frac{n}{2}+1}^{n} x_i),$$

and

$$h_n(x_1, x_2, \ldots, x_n) = (\sum_{i=1}^{\frac{n}{2}} x_i)(\sum_{\frac{n}{2}+2}^{n} x_i)$$

Similarly, the ANFs of a_n and b_n are

$$a_n(x_1, x_2, \ldots, x_n) = (\sum_{i=1}^{\frac{n}{2}} x_i)(1 + \sum_{i=\frac{n}{2}+1}^{\frac{n}{2}} x_i)$$

and

$$b_n(x_1, x_2, \ldots, x_n) = f_{\frac{n}{2}}(x_1, x_2, \ldots, x_{\frac{n}{2}}) \prod_{i=1}^{\frac{n}{2}} (x_i + x_{\frac{n}{2}+i} + 1)$$

Therefore,

$$\bar{f}_n(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{\frac{n}{2}} x_i + \sum_{i=1}^{\frac{n}{2}} x_i \sum_{\frac{n}{2}+2}^{n} x_i + \bar{f}_{\frac{n}{2}}(x_1, x_2, \ldots, x_{\frac{n}{2}}) \prod_{i=1}^{\frac{n}{2}} (x_i + x_{\frac{n}{2}+i} + 1)$$

□

The k-weightwise nonlinearity of the WAPB functions f_6, f_7 and f_9 are given in 1, 2 and 4 respectively.

5 Conclusions and Future work

We have presented a construction of a class of WAPB Boolean functions in n-variable from the support of another WAPB Boolean function in n_0-variable, where $n_0 < n$. This construction generalizes a construction of WPB functions presented by Mesnager and Su [MS21]. We further have modified the construction for improving the k-weightwise nonlinearity. For future work, we will study some other cryptographic properties of this class of functions and construction of WAPB Boolean functions.

WPB/ WAPB functions	$\mathtt{nl}$	$\mathtt{nl}_2$	$\mathtt{nl}_3$	$\mathtt{nl}_4$
Upper Bound [CMR17]		5	7	5
Carlet, Méaux and Rotella [CMR17]	-	2	4	2
Zhu and Su [ZS22, f_n equation(8)]	-	1	4	1
Construction 1				

Table 1: Weightwise nonlinearity $\mathtt{nl}_k$ of 6-variable WAPB constructions.

WPB/ WAPB functions	$\mathtt{nl}$	$\mathtt{nl}_2$	$\mathtt{nl}_3$	$\mathtt{nl}_4$	$\mathtt{nl}_5$
Upper Bound [CMR17]		8	14	14	8
Zhu and Su [ZS22, f_n equation(8)]	-	1	5	5	1
Construction 1					

Table 2: Weightwise nonlinearity $\mathtt{nl}_k$ of 7-variable WAPB constructions.

WPB/ WAPB functions	$\mathtt{nl}$	$\mathtt{nl}_2$	$\mathtt{nl}_3$	$\mathtt{nl}_4$	$\mathtt{nl}_5$	$\mathtt{nl}_6$
Upper Bound [CMR17]	120	11	24	30	24	11
Carlet, Méaux, Rotella [CMR17]	-	2	12	19	12	2
Li and Su [LS20, $g_{2^{q+2}}$ equation(9)]	-	2	12	19	-	-
Mesnager and Su [MS21, f_m equation(13)]	-	2	0	3	0	2
Mesnager and Su [MS21, g_m equation(22)]	-	2	14	19	14	2
Mesnager, Su and Li [? , f_m equation(2)]	-	2	8	8	8	2
Mesnager, Su and Li [? , f_m equation(3)]	-	6	8	26	8	6
Zhang and Su [? , g_m equation(11)]	-	2	12	19	12	6
Construction 1						

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

WPB/ WAPB functions	n	$\mathtt{nl}$	$\mathtt{nl}_2$	$\mathtt{nl}_3$	$\mathtt{nl}_4$	$\mathtt{nl}_5$	$\mathtt{nl}_6$	nl_7
Upper Bound [CMR17]			15	37	57	57	37	15
f_n in equation (5)	9	-	-	-	-	-	-	-
	10	-	-	-	-	-	-	-
	11	-	-	-	-	-	-	-
	12	-	-	-	-	-	-	-
	13	-	-	-	-	-	-	-
$\bar{f}_n$ in equation (**??**)	9	-	-	-	-	-	-	-
	10	-	-	-	-	-	-	-
	11	-	-	-	-	-	-	-
	12	-	-	-	-	-	-	-
	13	-	-	-	-	-	-	-

Table 4: Weightwise nonlinearity $\mathtt{nl}_k$ of WAPB construction-1.

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.

[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.

[Gou72] H.W. Gould. *Combinatorial Identities: A Standardized Set of Tables Listing 500 Binomial Coefficient Summations*. Gould, 1972.

[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.

[Luc78] Édouard Lucas. Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques suivant un module premier. *Bulletin de la Société mathématique de France*, 6:49–54, 1878.

[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.

[MMM$^+$20] Subhamoy Maitra, Bimal Mandal, Thor Martinsen, Dibyendu Roy, and Pantelimon Stanica. Analysis on boolean function in a restricted (biased) domain. *IEEE Transactions on Information Theory*, 66(2):1219–1231, 2020.

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

[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.