# A Class of Weightwise Almost Perfectly Balanced Boolean Functions

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, HBNI,
Bhubaneswar, Odisha 752050, India
Email: {deepak, krishna.mallick}@niser.ac.in

**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.

***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, '+' symbol is used for the addition operation in both $\mathbb{F}_2$ and $\mathbb{R}$. Generally, the cryptographic criteria of the Boolean functions 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]. In this stream cipher, the Hamming weight of the inputs to the filter function is $\frac{n}{2}$.An initial cryptographic study of Boolean function in a restricted domain is introduced by Carlet et al. in [CMR17]. The Boolean 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 first weightwise perfectly balanced (WPB) Boolean function construction was introduced in [CMR17] in 2017. Two constructions of WPB Boolean functions are presented in [MS21] by modifying the support of linear and quadratic functions.

## 2 Preliminaries

Let $\mathcal{B}_n$ be the set of all $n$-variable Boolean functions. Let denote $[i, j] = \{i, i+1, \ldots, j\}$ for two integers $i, j$ with $i \leq j$. 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 $\mathcal{E}_n$ 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 $\mathtt{sup}_k(f) = \{v \in E_{n,k} : f(v) = 1\}$

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 $\mathtt{d}(f,g) = |\{v \in \mathbb{F}_2^n : f(v) \neq g(v)\}| = \mathtt{wt}(f+g)$. The truth table representation of a Boolean function $f \in \mathcal{B}_n$ is the $2^n$-tuple 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 $f(x) = \sum_{u \in \mathbb{F}_2^n} a_u x^u$, where $a_u \in \mathbb{F}_2$ and $x^u = x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n}$ for $x = (x_1, x_2, \ldots, x_n)$. 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 $\deg(f) \leq 1$, 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 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 almost perfectly balanced (WAPB) if, for $k \in [0,n]$, $\mathtt{wt}_k(f) = \frac{\binom{n}{k}}{2}$ 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, $\mathtt{nl}_k(f) = \min_{g \in \mathcal{A}_n} d_k(f,g) = \min_{g \in \mathcal{A}_n} \mathtt{wt}_k(f+g)$.*

**Proposition 2.4.** *[MS21] For a positive integer $n = 2^m$, the support of $f_n \in \mathcal{B}_n$ is defined by*

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

*Then the Boolean function $f_n$ is a WPB.*

The construction proposed in Proposition 2.4 is important for our study as we will provide a construction that generalizes it.

# 3 A class of WAPB Boolean functions

We provide several constructions for $n$-variable of WAPB Boolean functions in this section. In the paper [MS21], Mesnager and Su have proposed a WPB Boolean function over $n = 2^m$ variables using an iterative method (see 2.4) to build its support. Following lemmas are required to construct an $n$-variable WAPB from the support of another $n_0$-variable WAPB.

**Lemma 3.1.** *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*

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

$$\text{i.e., } \mathtt{sup}(f) = \{(x,0) \in \mathbb{F}_2^n : x \in \mathtt{sup}(g)\} \cup \{(y,1) \in \mathbb{F}_2^n : y \in \mathtt{sup}(h)\}$$

*is a WAPB Boolean function.*

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

**Corollary 3.2.** *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*

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

*is a WAPB Boolean function.*

If $g = h$, then Lemma 3.1 is a case of the construction proposed in [ZS22] for $n = 2^m + 1$. Further, if we take $h = 1 + g$ in the Lemma 3.1 then the following corollary is useful for our main construction.

**Corollary 3.3.** *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*

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

*is a WAPB Boolean function.*

**Lemma 3.4.** *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*

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

*is a WAPB Boolean function.*

We can present a general construction for WAPB Boolean functions on any number of variables using the Corollary 3.3 and Lemma 3.4.

**Theorem 3.5.** *For $n \geq 2$, the support of an $n$ variable Boolean function is defined as*

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

*is a WAPB Boolean function.*

When $n = 2^m$, 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 the destined Boolean function remains very poor. The construction in the Theorem 3.5 can be generalized for having good cryptographic properties from a base WAPB Boolean function on a higher variable.

**Theorem 3.6.** *For $p \geq 2$, let $f_p$ be a WAPB Boolean function. Let $n$ be a positive integer such that, for a $m \geq 0$,*

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

*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.*

### 3.1 Cryptographic Properties

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

**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 $m \geq 0$,*

- $p = \lfloor \frac{n}{2^m} \rfloor$ *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 3.6 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.*

Therefore, computation of the output of the function needs $O(\log_2 n)$ time complexity. The algebraic degree of $f_n$ can be computed as follows.

**Theorem 3.8.** *Let $f_p \in \mathcal{B}_p$ be a Boolean function with $\deg(f_p) \geq 1$ and $f_n \in \mathcal{B}_n$ constructed as in the Theorem 3.6. Then $\deg(f_n) = \lfloor \frac{n}{2} \rfloor + \lfloor \frac{n}{2^2} \rfloor + \cdots + \lfloor \frac{n}{2^m} \rfloor + \deg(f_p)$. 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.*

The Hamming weight of this class of Boolean functions can be computed using the following two Lemmas.

**Lemma 3.9.** *Let $n > 1$ be an odd integer and $f_{n-1} \in \mathcal{B}_{n-1}$ and $f_n \in \mathcal{B}_n$ Boolean function defined in Corollary 3.3. 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*

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

**Lemma 3.10.** *Let $n = n_0 2^m$ where $n_0$ be an odd positive integer and $m \geq 0$ be an integer. Let $f_{n_0} \in \mathcal{B}_{n_0}$ and $f_n \in \mathcal{B}_n$ are Boolean function defined in Lemma 3.4. For $k = k_0 2^b$, the $\mathtt{wt}_k(f_n) = \frac{1}{2}\left(\binom{n}{k} + a_k^n\right)$, where*

$$a_k^n = \begin{cases} 0 & \text{if } m > b, \\ a_{\frac{k}{2^m}}^{n_0} & \text{if } m < b, \\ -a_{\frac{k}{2^m}}^{n_0} & \text{if } m = b. \end{cases}$$

Further, since there are two different kinds of lifting in the recursive construction, we present the non-linearity bound for both cases.

**Lemma 3.11.** *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 $f_{n-1} \in \mathcal{B}_n$. Then $\mathtt{nl}(f_n) = 2\mathtt{nl}(f_{n-1})$.*

**Lemma 3.12.** *Let $n > 0$ be an even integer and $f_n \in \mathcal{B}_n$ such that*

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

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

If $f_{\frac{n}{2}}$ is a balance function, then $\mathtt{nl}(f_n) \leq \mathtt{wt}(f_{\frac{n}{2}}) = 2^{\frac{n}{2}-1}$. Therefore, the proposed construction has 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 in whether it is possible to get WAPB function by substituting the linear part with a very nonlinear part. Further, we have a discouraging result for weightwise nonlinearity.

**Corollary 3.13.** *If $n$ is even and $n > p$ then $\mathtt{nl}_k(f_n) = 0$ for all odd integer $k \in [0, n]$.*

The following table presents the nonlinearity and weightwise nonlinearity of the functions $f_n$ for $n = 10, 11, 12, 13, 14$, which are generated using the Theorem 3.5.

| $n$ | $\mathtt{nl}$ | $\mathtt{nl}_0$ | $\mathtt{nl}_1$ | $\mathtt{nl}_2$ | $\mathtt{nl}_3$ | $\mathtt{nl}_4$ | $\mathtt{nl}_5$ | $\mathtt{nl}_6$ | $\mathtt{nl}_7$ | $\mathtt{nl}_8$ | $\mathtt{nl}_9$ | $\mathtt{nl}_{10}$ | $\mathtt{nl}_{11}$ | $\mathtt{nl}_{12}$ | $\mathtt{nl}_{13}$ | $\mathtt{nl}_{14}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |

# 4 Conclusions and Future work

We have presented a construction of a class of WAPB Boolean functions in $n$ variables from the support of another WAPB Boolean function in $n_0$ variables, where $n_0 < n$. This construction generalizes a construction of WPB functions presented by Mesnager and Su [MS21]. We studied some cryptographic properties of the class of WAPB Boolean functions. The nonlinearity of this class of functions are very poor. For our future work, we will study some other cryptographic properties of this class of functions and construction of WAPB Boolean functions of good weightwise nonlinearity.

# 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.

[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.

[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.